

**An Advocacy Response to HUD's June 2005:
 "Domestic Violence Provider Participation in Homeless
 Management Information Systems (HMIS) Questions & Answers"**



<p>HUD Statements (June 2005)</p>	<p>National Network to End Domestic Violence Response & Clarification</p>
<p>1. What is the requirement for participation in HMIS according to the Data and Technical Standards Final Notice (the Notice) (69 FR 45888) and Domestic Violence Provider Clarification (the Clarification) (69 FR 61617)?</p> <p>HUD developed the draft and final HMIS Data and Technical Standards in consultation with domestic violence providers, advocates and other stakeholders. HUD has also provided clarification on how domestic violence providers can participate in HMIS based on feedback from local communities. The clarification mandates greater safety and confidentiality for domestic violence providers by allowing additional layers of protection, including use of masked identifiers in lieu of name and social security number and delayed entry of client records until after the clients exit the program.</p>	<p>The question asks about the requirement for participation; the answer is not responsive, and instead suggests that HUD consulted with domestic violence providers and that such consultation has led to greater protections for domestic violence victims than there would have been otherwise. In fact, in the proposed HMIS standards released July 2003, HUD stated that it was "aware of, and sensitive to, the data confidentiality and security concerns" of domestic violence victims and therefore provided a critical domestic violence exemption.ⁱ</p> <p>In the final HMIS standards, HUD acknowledged that it "understood that unlike other special populations, victims of domestic violence could be physically at risk if individuals who intend to cause them harm are able to obtain personal information from an HMIS."ⁱⁱ Even after acknowledging this risk, HUD removed the Domestic Violence Exemption in the final HMIS standards,ⁱⁱⁱ without any consultation with national or state domestic violence organizations.</p> <p>Contrary to HUD's inference, almost every one of the 167 separate HMIS comment submissions of 2003 supported the Domestic Violence Exemption. HUD's reversal and elimination of the Exemption, which would provide the highest level of protection for victims of domestic violence, was a complete surprise to advocates nationwide.</p> <p>HUD also states, in the Clarification, that "[I]n the event that state laws conflict with the Final Notice, as determined by an appropriate state government entity, state law will prevail." The accurate answer to HUD's first "FAQ" under its own Clarification should therefore be that the requirement for participation in HMIS is subject to state law confidentiality requirements, and programs must honor victim confidentiality above HUD's data collection.</p> <p>*Note, delayed entry does not protect victims since they are at an increased risk of harm after separation from an abusive partner.^{iv} Many victims flee to a shelter and then attempt to relocate permanently into the same community. It is critical that shelters protect a victim's new location even after she has exited.</p>
<p>2. What is the timing for participation for domestic violence providers in HMIS?</p> <p>CoCs may stage the entry of domestic violence providers last into their local HMIS to allow adequate time for planning and implementing the privacy and security measures presented in the final HMIS Notice. There is no set deadline for domestic violence providers to participate in local HMIS systems. Instead, Continuum of Care representatives are instructed to meet with domestic violence providers to establish protocols that would protect the safety of domestic violence survivors.</p>	<p>Under HUD's own terms, there is no stated deadline for program participation, and funding should not be threatened or lost for domestic violence programs that do not participate in HMIS at this point. However, domestic violence programs around the country are being inappropriately pressured to provide confidential and life-threatening victim information or risk losing critical HUD funding. Further, programs that provide confidential victim information could be in violation of state law, and face liability for disclosure of personal information.</p>
<p>3. How does HMIS protect individual safety and confidentiality for victims of domestic violence?</p> <p>Protection of information for all clients who are entered into a local HMIS, including victims of domestic violence, is an essential requirement of HMIS. The Notice sets very high</p>	<p>Entering any victim-level information into a HMIS system could breach victim confidentiality and privilege. Over 30 state laws and several federal laws prohibit sharing victim information into these 3rd party databases.</p>

<p>baseline privacy and security standards for all users of HMIS to protect personal information collected from all homeless clients. These standards require, at a minimum, eight layers of security and privacy protections that were lacking prior to the release of the final HMIS Notice. These layers include strict user authentication measures, firewalls, digital certificates, system monitoring requirements, restrictions on physical access, protections for hard copy data, and provisions that significantly restrict the uses and disclosures of personal information. The minimum standards for HMIS are more stringent than other mainstream systems that collect and store client data for receipt of welfare, food, or other social services.</p>	<p>While computer security is one important element of any database, even if all of these eight layers are achieved, victims will still be in danger from internal abusers who work for the government or law enforcement, and victim’s legal confidentiality will be compromised by the HMIS human tracking system.</p> <p>Most non-profit organizations do not have full time system administrators on staff and experience high staff turnover. Given these conditions, it is highly likely that victim information in these invasive tracking systems will be vulnerable.</p> <p>It is not possible to compare emergency abuse shelters to optional social services. Many victims who are fleeing for their lives are not able to safely access these optional services because having their information shared beyond the shelter walls could be deadly. Taking away the ability for victims to safely and anonymously hide in a domestic violence shelter would be unconscionable.</p>
<p>4. What do the HMIS standards do to prevent unauthorized users from accessing confidential client information?</p> <p>Communities must implement numerous provisions that prevent unauthorized access to any client data and must also monitor access on a regular basis. Each user of the system must be authorized to access the HMIS and must sign a confidentiality agreement to protect clients’ privacy and prevent unauthorized access to the system. The baseline security standards also control the location of, and access to, any computer accessing a local HMIS system by requiring: HMIS and workstation usernames and passwords; locking screen savers; session timeouts; virus protection; firewalls; location control; public access controls; and system monitoring. Public access control is a very stringent standard that is not required by many other systems that collect and store client data. The standard requires public access to be controlled through VPN (Virtual Private Network), static IP (Internet Protocol) address or digital certificates (PKI- Public Key Infrastructure) that are installed on all computers that can connect to the HMIS. These access controls can be regulated and monitored by the HMIS administrator. Public access controls prevent access to client data by preventing unauthorized computers from even gaining access to the HMIS login page.</p>	<p>While HUD makes an attempt to address the process of securing data from unauthorized users, HUD has never addressed the extremely unfortunate reality that over half^v of all security breaches occur from inside an organization and that victims are at risk from someone who works for the local CoC, computer company, or law enforcement organization.</p> <p>From February to July 2005, almost 50 million people have been affected by security breaches at companies with extremely skilled and well funded technology security departments.^{vi}</p> <p>If private industry cannot guarantee data security, how can we expect under-funded and under-staffed non-profit organizations to do so?</p>
<p>5. Does the Final Notice require data sharing among providers participating in HMIS?</p> <p>No, the Notice does not require sharing of HMIS data among providers within the CoC, rather it is left to the discretion of each CoC and its providers to develop policies and protocols for appropriate data sharing. However, the CoC is required to aggregate all agency data at least once a year for the purposes of reporting, providing an unduplicated count, analyzing service utilization patterns, and measuring system effectiveness measures.</p>	<p>HUD and many CoCs are using the term “sharing” in a somewhat unique fashion. ALL HMIS systems are requiring that battered women’s shelters eventually “SHARE” confidential victim information to 3rd party databases, therefore violating legal and advocate privilege.</p> <p>HUD, HMIS vendors, and many CoCs use “sharing” to mean optional access levels that vendors can use to limit which other community agencies can view the sensitive victim information that has already been shared into the central HMIS server and is thus vulnerable to subpoena, hacking, and abusers who work for the system.</p>
<p>6. How can conformance with the Notice be monitored?</p> <p>The Notice requires that every Covered Homeless Organization (CHO) comply with stringent privacy and security protocols. HUD has developed technical assistance documents that provide guidance on how to monitor conformance with the data standards and is presently providing comprehensive training to educate local CoC grantees and sponsoring agencies. The trainings focus on conformance with, and implementation of, the baseline data collection, privacy, and security requirements.</p>	<p>Since HUD is not addressing internal abusers and perpetrators using other legitimate means to access HMIS data, even if all HMIS “privacy and security” requirements are met, victims are still at significant risk.</p> <p>It is the unfortunate reality that true conformance may not be known until a victim of domestic violence is tracked down by her perpetrator accessing her location in a HMIS database, and her surviving family members sue the local shelters, Continuum of Care,</p>

<p>7. How do the HMIS Final Notice and Clarification handle state and local laws?</p> <p>HUD recognizes that state law may affect a provider's ability to comply with the Final Homeless Management Information Systems (HMIS) Data and Technical Standards. As stated in Section 4 of the Final Notice and reiterated in the Clarification and Additional Guidance on Special Provisions for Domestic Violence Provider Shelters, 69 FR 61517 (10/19/04) ("the Clarification"), organizations must also comply with federal, state and local laws that require additional confidentiality protections. HUD directed that state law would prevail in the event a conflict exists between state law and the HMIS standards "as determined by an appropriate state government entity." HUD Office of General Counsel has determined that the appropriate state government entity to make such a determination is the Attorney General of the state.</p> <p>Communities should request the Attorney General of their state/commonwealth to prepare and submit to HUD a legal opinion with regard to the effect of local law. Only one opinion will be required for each state or commonwealth. The opinion must:</p> <ol style="list-style-type: none"> 1) Cite the documents, statutes, case law, rules and regulations upon which the Attorney General relied in issuing the opinion; 2) Identify the specific conflict(s) between the HMIS standards and state law; 3) Address why the approach described in the Clarification (e.g., use of a proxy, coded, encrypted, or hashed unique identifier) does not resolve the conflict with state law; 4) Address why obtaining client consent does not resolve the conflict with state law; 5) Explain the reason underlying the conclusion that providers are prohibited from complying with HMIS standards; and 6) State that HUD may rely upon the opinion. <p>HUD will begin its consideration of requests to recognize that state law precludes compliance with HMIS standards only upon receipt of the Attorney General's opinion.</p>	<p>and others who put the victim's location at risk.</p> <p>HUD continues to change the method and criteria for determining the meaning of state laws governing confidentiality.</p> <p>Originally, HUD stated that communities should comply with federal, state and local laws that require additional confidentiality protections. (Final Standards released July 30, 2004).</p> <p>Then as states across the country began sending legal memos to HUD explaining how their state laws prohibited domestic violence programs from providing victim information to HMIS systems, HUD "clarified" the process and stated that "in the event that state laws conflict with the Final Notice, as determined by an appropriate state government entity, state law will prevail" (HUD Clarification, October 15, 2004)</p> <p>As more and more state entities sent legal memos to HUD articulating the state law conflict, HUD changed the criteria in their June 2005 memo. HUD is now requiring state Attorneys General to determine if their own state laws require that victim information be kept confidential. State Attorneys General around the United States are extremely concerned about victim safety, and understand the legislative intent of the victim confidentiality laws is indeed to protect victim information. Therefore, the Attorneys General of many states have already begun sending new memos to HUD to address HUD's latest requirements. Remarkably, HUD seems to suggest that it may second-guess the Attorney General's interpretation of its own state law.</p>
<p>8. Why is HUD requiring communities to implement Homeless Management Information Systems?</p> <p>Every HUD appropriation bill since 2001 included funding for HMIS and was accompanied by Congressional direction to HUD, Congress has directed HUD to generate an unduplicated count of clients served at the local level; analyze patterns of service use and assistance; and evaluate the effectiveness of the homeless services system. Congress has required HUD to both develop a strategy for improving homeless data collection, reporting and analysis and to report on the departments progress annually.</p> <p>Additionally, the experiences of several communities that have long-standing HMIS demonstrate that these systems are an effective tool for reducing and preventing homelessness among all populations. Good local data assists communities to make informed decisions about the most effective service delivery models for people who are homeless.</p>	<p>In 2001, the Veterans' Affairs, Housing and Urban Development Appropriations Conference Committee directed the Department of Housing and Urban Development (HUD) to collect data on the extent of homelessness at a local level.^{vii} This directive was intended to provide a more truly unduplicated count of homeless persons and to understand how to meet their needs effectively.</p> <p>Broadly interpreting this laudable directive, HUD proposed federal standards to require HUD-funded entities to implement local Homeless Management Information Systems (HMIS), complex databases for collecting, tracking and sharing comprehensive personally identifiable data about individuals who use services for the homeless, including battered women. HUD chose the HMIS model out of many possible methods of better measuring the extent of homelessness.</p>
<p>9. Are domestic violence agencies currently participating in HMIS?</p> <p>Yes. Many domestic violence providers have been fully engaged with their local HMIS and have developed protocols for protecting the privacy of their clients. Communities in Washington and Ohio have had long standing participation by domestic violence shelters with no incidents or breeches of client confidentiality. As a result, these communities have been able to address the needs of domestic violence victims more effectively by quickly linking them to the resources needed to move them into stable and safe housing.</p>	<p>While HUD states in this June 2005 document and in media interviews that "many" domestic violence agencies are participating, further examination and survey shows that very few domestic violence shelters have been participating in HMIS, and those few, under duress or from misinformation.</p> <p>In most states no more than 1 or 2 domestic violence shelters (out of 60-90 in a state) may have been convinced that the victim information would be held confidential, not understanding that legal advocate privilege is compromised and that state law may prohibit</p>

	<p>submitting victim information. In a few other cases, domestic violence shelters were threatened with sweeping funding losses and may have given some limited victim information before learning that they are not required to break state laws.</p>
<p>10. Can HUD achieve the congressional goal of obtaining an unduplicated count of homeless persons through point-in-time counts or anonymous databases?</p> <p>No. Point-in-time counts provide a crude “snapshot” of homelessness and fail to provide a full understanding of the nature and extent of homelessness in a community. Point-in-time counts are especially ineffective in understanding homelessness among subpopulations that access the homeless service system irregularly and may not be present on the day of the point-in-time count, such as homeless families. Point-in-time counts also misrepresent service use patterns among individuals and families because this approach lacks the historical context provided by longitudinal HMIS data.</p> <p>Furthermore, CoCs cannot achieve an accurate unduplicated count of homeless persons without a unique identifier approach for each client. Traditional head counts drastically undercount persons that experience situational crisis, such as victims of domestic violence, and/or those persons that move in and out of the system regularly. As a result, communities will not be able to fully identify the needs of their homeless population and, in turn, will unknowingly under serve these clients.</p>	<p>Given a wide array of less expensive and more efficient survey options, HUD chose an expensive human tracking system that is far more invasive than Sexual Offender Registries which are used to monitor convicted felons, while HMIS is tracking innocent victims who are running for their lives.</p> <p>There are many viable options to collect better information about the extent of homelessness. While HUD is relatively new at gathering information on services and outcomes, domestic violence programs and indeed many local community programs have demonstrated long histories of collecting and reporting sophisticated unduplicated counts of clients using their own services.</p> <p>In addition there are creative methods of addressing community wide counts without compromising the safety of even one victim or compromising the human dignity of even one citizen. Those creative methods are not being employed here.</p>
<p>11. Why have some domestic violence shelters and their clients supported participation in Local Homeless Management Information Systems?</p> <p>The experiences of several communities with existing HMIS demonstrate the benefits to homeless persons, homeless service providers, and public policymakers interested in reducing and preventing homelessness. Understanding the needs of clients served by the network of service providers will enable domestic violence providers to identify the unmet needs of this population, advocate for additional resources, and coordinate services more effectively across the homeless assistance system.</p>	<p>There has been pressure from HUD for programs to participate, under a threat that those who do not participate will lose funding. Although HUD’s directives and Clarification indicate that domestic violence program participation is not required at this time, and that funding will not be lost because of non-participation, programs are now concerned that they will lose funding. Programs that support participation in local HMIS may be in the untenable position of complying with HUD demands for private information in violation of other state and federal laws.</p>
<p>12. What strategies are presently being used by local Domestic Violence Provider agencies participation in HMIS?</p> <p>Use of Hashed Identifiers1- Each DV provider agency or small DV provider network collects personally identifiable data at the program level and uploads the client data using a hashed identifier once a year to a central database. This aggregate database can be hosted and controlled by either a trusted research entity or a DV provider agency and is used to undertake annual analysis of client data, including generation of unduplicated counts.</p> <p>The hashing technique scrambles each personal identifier into a completely indecipherable value. Unlike standard encryption, the hashing process cannot be reversed, and there is no key to decrypt the hashed information. Hashing identifiers using the standard SHA-1 algorithm will allow communities to match records within the system without using personal identifiers. Hashing can be applied upon export from, or import to, a database as shown below.</p> <p>PIN Generator2: Denver’s HMIS implementation utilizes an application that creates a valid PIN for clients that require anonymity without the need to transmit, log, store or save personally identifying information into the HMIS. Client data (client’s name, social security number, data of birth, gender, and other pertinent information) are entered into a secure application (or applet) installed on an agency’s personal computer that generates a PIN using a series of propriety</p>	<p>HUD’s clarification states that “ HUD will not require the submission of personal identifiers from these programs to the CoC...” and that “domestic violence programs can choose to use a proxy, coded, encrypted, or hashed unique identifier—in lieu of name and SSN...” However, each of these options is based on a method, technological or manual, simple or complex, that would require that the domestic violence program compromise victim safety and confidentiality by releasing client identifying information, in part or in whole.</p> <p>Hashing techniques, coded identifier techniques, PIN generator techniques and similar proposed solutions, all scramble identifiers into what HUD sites as “completely indecipherable value”. However, this is untrue. Although these techniques vary slightly, they all function on the general principle of scrambling client identifying data. In each of these cases, the domestic violence program takes client’s identifiers, scrambles into another value and periodically uploads this scrambled value and related records to a central server HMIS. Each technique uses a different scrambling procedure, however all of these methods would still result in domestic violence programs in many states breaching their own state confidentiality statutes.</p> <p>Regardless of the specific identifier scrambling technique, there remain questions and issues regarding access to the definition, key,</p>

calculations. Once the PIN is generated, the personal information is gone - it is not stored, logged, or transmitted. [To comply with the HMIS Data and Technical Standards clarification, agencies must maintain hard copies of this information.] The PIN Generator also calculates an accuracy rating based on the completeness of each data field. PIN numbers that are similar and which share a high accuracy rating can be used to provide non-duplicated data counts for HMIS reporting across the community. The PIN protects clients' identity beyond the HMIS privacy and security requirements. In the event that an unauthorized user gains access to the data, or if the data are subpoenaed, personally identifying information cannot be retrieved because it was never entered into the database. Theoretically, this solution is only acceptable for domestic violence shelters and not recommended for clients generally.

or "code" to decipher the scrambled identifier. Currently, several people would have access to the definitions of scrambled identifiers. Anyone using the hashing technique or anyone with access to these hashing definitions at the CoC, can then access the client identifiers of any record stored within the HMIS if that person had authorized or unauthorized access to the HMIS. This hashing solution would therefore cause domestic violence programs to breach state confidentiality statutes by allowing someone outside of the domestic violence program to have access to client identifying information.

Encryption techniques are used to keep data more secure while in transit from an agency and/or once it arrives at a central server HMIS. **Continued below**

Continued Advocacy Clarification

Encryption techniques are neither intended nor able to prevent the release of client information from a domestic violence program. While encryption may keep data released by the domestic violence program more secure, the domestic violence program would still be releasing this information to others outside of the domestic violence program, which is prohibited by over 30 state laws. In this example, a computer programmer writes the encryption algorithm, the "how is the computer going to "lock down" the information that is stored". Minimally that same programmer will know how to unencrypt or "unlock" the information to view the data that is being transmitted or stored, including client identifiers. Therefore, third parties (at minimum, this programmer) would be able to obtain the identifiers that are being stored in that system, in part or in whole. This encryption solution would therefore cause DV programs to breach state confidentiality statutes, by allowing someone outside of the domestic violence program to have access to client identifying information. In this type of system, the CoC would be able to get an unduplicated count because the client identifiers are in fact stored on the central server.

Denver's PIN Generator retains personally identifying information about victims, therefore it would still breach state confidentiality laws. The Denver PIN method contains a "Birth Date and Gender Extractor"^{viii} that allows "authorized HMIS Continuum of Care staff" to pull out those two data elements. This contradicts the HUD FAQ statement that "personally identifying information cannot be retrieved because it was never entered into the database."

"87% of the population in the United States had reported characteristics that likely made them unique based only on **5-digit ZIP, gender, and date of birth**. About half of the U.S. population (132 million of 248 million or 53%) are likely to be uniquely identified by only **place, gender, date of birth**."^{ix}

Example (PIN generators and hashing techniques may vary) A HMIS system could use a coding system where Sarah Smith is coded as 12345 at Agency 1, Sarah Smith is coded as 12345 at Agency 2, etc. Then at the central server there would be several records with the same scrambled identifiers or 12345. If some DV programs enter Sarah as 12345 and other homeless providers enter her as "Sarah Smith", all of her information would still be linked in the central server. It would be possible to identify Sarah by a) seeing her demographics – how many children she has, their ages, etc; b) entering Sarah's information into the computer to see what her code number would be; c) subpoenaing the information since her date of birth and other identifying information could be de-coded with the encoding formula.

ⁱ Department of Housing and Urban Development's Homeless Management Information Systems ("HMIS") Data and Technical Standards, Docket No. FR 4848-N-01. 43430 Federal Register / Vol. 68, No. 140 / Tuesday, July 22, 2003 / Notices Page 43435

ⁱⁱ Federal Register / Vol. 69, No. 146 / Friday, July 30, 2004 / Notices. Department of Housing and Urban Development Homeless Management Information Systems (HMIS); Data and Technical Standards Final Notice Page 45891

ⁱⁱⁱ Federal Register / Vol. 69, No. 146 / Friday, July 30, 2004 / Notices. Department of Housing and Urban Development Homeless Management Information Systems (HMIS); Data and Technical Standards Final Notice Page 45902

^{iv} Ronet Bachman and Linda Salzman, Bureau of Justice Statistics, *Violence Against Women: Estimates From the Redesigned Survey* 1 (Jan 2000).

^v CSI/FBI 2003 Computer Crime and Security Survey, Computer Security Institute, Page 7

^{vi} Privacy Rights Clearinghouse. **A Chronology of Data Breaches Reported Since the ChoicePoint Incident**, Posted: April 20, 2005, Updated July 11, 2005 <http://www.privacyrights.org/ar/ChronDataBreaches.htm>

^{vii} (H.R. Report 106-988; Senate Report 106-410). "Local jurisdictions should be collecting an array of data on homelessness in order to prevent duplicate counting of homeless persons, and to analyze their patterns of use of assistance, including how they enter and exit the homeless assistance system and the effectiveness of the systems."

^{viii} VisionLink HMIS Universal PIN Generator. **Guaranteeing Client Anonymity and Non-Duplicated Services & Reporting**. "For authorized HMIS Continuum of Care staff, a special module allows client birth dates and gender to be extracted from the secure algorithm, for the purposes of minimal reporting and data analysis." Page 4

^{ix} L. Sweeney. *Uniqueness of Simple Demographics in the U.S. Population*, LIDAP-WP4. Carnegie Mellon University, Laboratory for International Data Privacy, Pittsburgh, PA: 2000. Abstract. <http://privacy.cs.cmu.edu/dataprivacy/papers/LIDAP-WP4abstract.html>