

Domestic Violence Provider Participation in Homeless Management Information Systems (HMIS)

Questions & Answers

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)?

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.

2. What is the timing for participation for domestic violence providers in HMIS?

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.

3. How does HMIS protect individual safety and confidentiality for victims of domestic violence?

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 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.

4. What do the HMIS standards do to prevent unauthorized users from accessing confidential client information?

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.

5. Does the Final Notice require data sharing among providers participating in HMIS?

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.

6. How can conformance with the Notice be monitored?

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.

7. How do the HMIS Final Notice and Clarification handle state and local laws?

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 (Pg. 45928) 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.

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:

- 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.

The opinion is to be addressed to the Secretary of HUD, and mailed to:

Elton J. Lester, Assistant General Counsel
Office of Assisted Housing and Community Development
U.S. Department Of Housing and Urban Development
451 Seventh Street, SW, Room 8158
Washington, D.C. 20410.

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. Questions from the Offices of the Attorney General should be referred to Lynn Morgan, Senior Attorney, Office of General Counsel, Community Development Division, at 202-708-2027.

8. Why is HUD requiring communities to implement Homeless Management Information Systems?

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. These annual reports can be found at <http://www.hud.gov/offices/cpd/homeless/hmis/strategy/index.cfm>.

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.

9. Are domestic violence agencies currently participating in HMIS?

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.

10. Can HUD achieve the congressional goal of obtaining an unduplicated count of homeless persons through point-in-time counts or anonymous databases?

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.

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.

11. Why have some domestic violence shelters and their clients supported participation in local Homeless Management Information Systems?

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.

12. What strategies are presently being used by local Domestic Violence Provider agencies participation in HMIS?

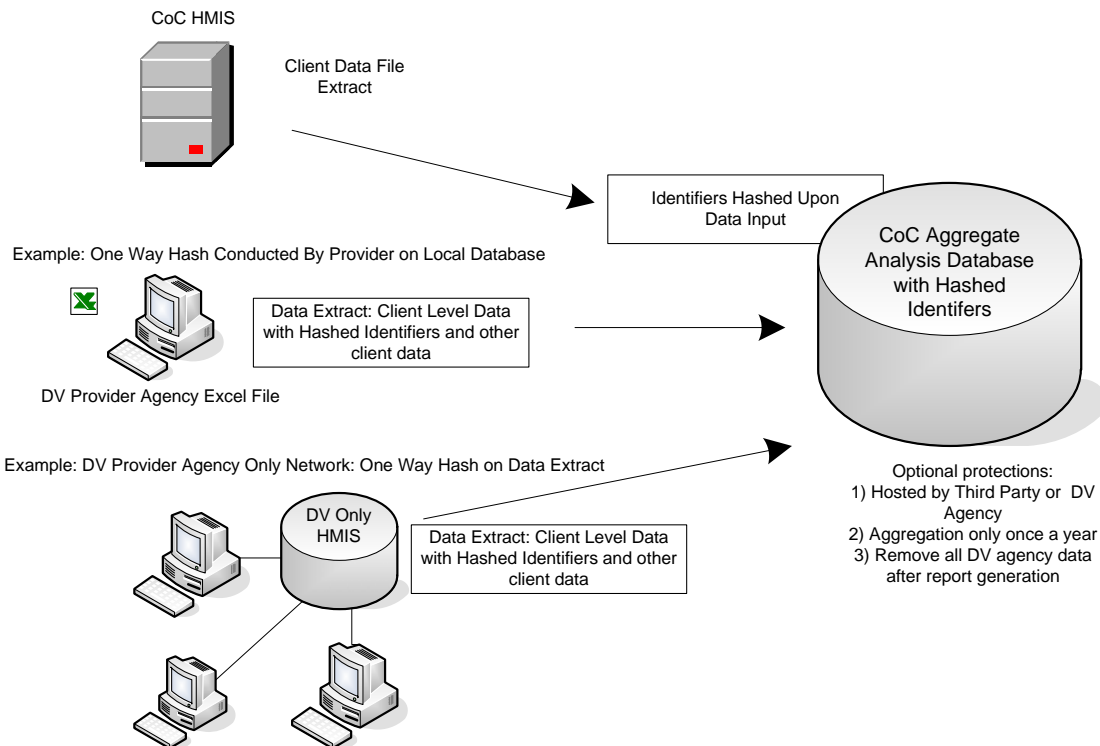
Use of Hashed Identifiers¹ - Each DV provider agency or small DV provider network collects personally identifiable data at the program level and uploads the client data using a hashed identifier once a year to a central database. This aggregate database can be hosted and controlled by either a trusted research entity or a DV provider agency and is used to undertake annual analysis of client data, including generation of unduplicated counts.

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.

Example of the Hashing Process:

Original Value	Hashed Value
SSN: 555555555	ea81f98936c00666d1e9dae66a2d2166
Last name: Sullivan	adb831a7fdd83dd1e2a309ce7591dff8

Domestic Violence Provider Agency Participation Examples



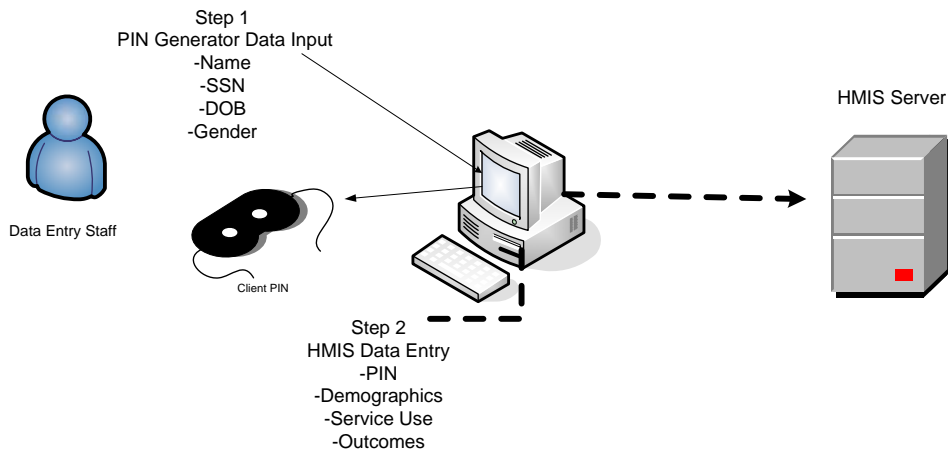
Note: this diagram does not visually depict additional minimum privacy and security requirements of HMIS

¹ For more information, reference the upcoming release by the Center for Social Policy, UMass Boston (by June 2005) Technical Guidelines for De-identifying and Unduplicating HMIS Client Records. Additional information on the SHA-1 standards is available at <http://csrc.nist.gov/CryptoToolkit/tkhash.html>.

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 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.

HMIS Computer with PIN Generator Applet Installed on Local PC



Note: this diagram does not visually depict additional minimum privacy and security requirements of HMIS

² Information was obtained from VisionLink, Inc. Additional information is available on their website at www.visionlink.org.