

MEMORANDUM

TO: Regional Steering Committee on Homelessness and Housing

FROM: HomeBase

DATE: January 23, 2009

RE: Search Warrants and HMIS Disclosures

I. Brief Summary

The Regional Steering Committee on Homelessness and Housing (RSC) has taken an interest in Homeless Management Information Systems (HMIS) since its introduction. RSC views on HMIS issues are informed by many years of experience as members have contributed to numerous regional and state meetings and conferences on technology, information sharing, and confidentiality. The RSC addressed the general topics of confidentiality and security in 1994 via a workshop called “Housing California Confidentiality of Client Information” and then revisited the issues through papers presented in 1995 entitled “Legal and Policy Issues in Shared Client Information” and “Confidentiality of Client Information.” In 1998, the RSC was given a presentation entitled “Homeless Services Information Management Systems.” Then, in September 2001, the group reviewed best practices and design steps communities needed to take to implement and expand HMIS. Throughout 2002 and 2003, the RSC remained informed of various workshops and conferences as communities began to implement HMIS. In 2003, the RSC analyzed the Draft National Uniform HMIS Standards, prepared feedback on the Standards, then continued to track the Standards once officially published in 2004. The Department of Housing and Urban Development (HUD) sponsored a series of meeting to gather input and assist in implementation. Regional data work continues with the Bay Area Counties Homeless Information Collaborative (BACHIC). The last memorandum presented to the RSC pertaining to HMIS was in October 2008 entitled “HMIS Changes in the Works.”

The present memorandum is intended to provide greater understanding and guidance for homeless service organizations participating in HMIS regarding the rights and responsibilities that exist when confronted with a search warrant from a law enforcement officer for HMIS information. Please note that this memorandum is general in nature and specific situations concerning criminal investigations should always be examined on a case-by-case basis in order to best assess all parties’ rights and duties. With this in mind, the following section provides the basics on search warrants.

Have you experienced a situation where law enforcement officers sought HMIS information?

Have you experienced a situation where law enforcement officers sought to execute a search or arrest warrant at your organization?

Do you have any opinions, concerns or advice on how best to address a situation that involves privacy concerns, law enforcement activity and/or HMIS?

II. The Basics On Warrants

The Fourth Amendment to the U.S. Constitution, which protects citizens from unreasonable searches and seizures by the government, regulates search warrants. Law enforcement officers investigating a crime must draft two documents in order to obtain a search warrant from a judge or magistrate:

1. An affidavit, which is a sworn statement by the investigating officer that explains the basis for the belief that the search is justified by “probable cause”¹. A well-drafted affidavit should include an explanation of the search strategy, when relevant to the circumstances.
2. The proposed warrant itself that describes the place to be searched and the persons or things to be seized.

If a judge agrees that the affidavit establishes probable cause and the proposed warrant describes in enough specificity the place to be searched and the things to be seized then the judge will sign the warrant. Law enforcement officers must execute the warrant within ten (10) days after being signed by the judge.²

It is the independent judge who balances the investigative merits of a case being worked on by the law enforcement officers against the constitutional privacy interests of the citizens. The next section explores the rules and regulations associated with HMIS data.

¹ In determining what is probable cause for a search warrant a court is concerned with the question whether the affiant [law enforcement officer] had reasonable grounds at the time of his affidavit to believe that the law was being violated and if the facts set out in the affidavit are such that a reasonably prudent person would be led to believe that there was a commission of the offense charged. *Dumbra v. United States*, 268 U.S. 435, 439 (1925).

² See: Fed. R. Crim. P. 41(b).

III. The Federal Register – An Authority

The Federal Register is the official daily publication for rules, proposed rules, and notices of federal agencies and organizations, as well as executive orders and other presidential documents. The Federal Register is published by the Office of the Federal Register within the National Archives and Records Administration (NARA)³ and it could be described as the official journal of the United States Government as it contains most of the routine publications and public notices.

The Department of Housing and Urban Development (HUD) published in the Federal Register the HMIS Data and Technical Standards Final Notice on July 30, 2004.⁴ HUD developed the HMIS national data standards for three primary reasons. First, the data standards provide clarity for the types of information collected by local homeless assistance providers to ensure that providers are collecting the same types of information consistently. Second, the national standards help further standardize reporting across federal programs and across other funders of programs for the homeless. Finally, the HMIS standards assist communities in implementing uniform privacy and security provisions to adequately protect client confidentiality. The national standards include privacy and security requirements that are a significant improvement over past practices, set high baseline standards for all users of HMIS data, and provide important safeguards for personal information collected from all homeless clients.⁵

IV. The Two-Tiered Approach To Managing Client Data

In managing HMIS information, especially for protected personal information (PPI)⁶, there exists a two-tiered approach. This approach includes a baseline level, with which a covered homeless organization (CHO)⁷ must comply, and optional additional levels of privacy protections. This two-tiered approach is designed to recognize the many types of programs and organizations that participate in HMIS and the realities they face. Some organizations, such as those serving victims of domestic violence, may choose to implement higher levels of privacy and security standards than the minimum baseline requirements due to the nature of their homeless population and/or service provided. Others may find standards above the baseline burdensome or impractical. At a minimum, however, all organizations must meet the baseline privacy and security requirements.

³ See: <http://www.gpoaccess.gov/fr/about.html>.

⁴ See: 69 Fed. Reg. 45888 et. seq. (7-30-2004).

⁵ Homeless Management Information Systems: Frequently Asked Questions, July 2005, p. 1.

⁶ Protected Personal Information (PPI): Any information maintained by or for a Covered Homeless Organization about a living homeless client or homeless individual that: (1) Identifies, either directly or indirectly, a specific individual; (2) can be manipulated by a reasonably foreseeable method to identify a specific individual; or (3) can be linked with other available information to identify a specific individual. 69 Fed. Reg. 45928 (7-30-2004).

⁷ Covered Homeless Organization (CHO): Any organization (including its employees, volunteers, affiliates, contractors, and associates) that records, uses or processes PPI on homeless clients for an HMIS. 69 Fed. Reg. 45928 (7-30-2004).

The July 30, 2004 Federal Register establishes baseline minimum privacy requirements for CHO's regarding the following topics:

Data Collection Limitations

- A CHO may only collect PPI when appropriate to the purpose for which the information is obtained or when required by law.
- Must use lawful and fair means and, where appropriate, with knowledge and consent of the client.
- Must post a sign in each intake area, or comparable location, and on the website (if applicable) explaining generally the reasons for collection of information.⁸

Data Quality

- Data collected must be relevant, accurate, complete, and timely for which it is used.
- Must have a plan to dispose, or remove identifiers from, PPI that is not in current use seven years after the PPI was created or last changed.⁹

Purpose and Use Limitations

- Must include in the privacy notice the purposes for data collection and all uses and disclosures.
- May only use or disclose PPI only as allowed by standards AND as described in the privacy notice.
- Uses or disclosures not specified in the privacy notice require consent (unless required by law).
- A CHO may infer consent for all uses and disclosures specified in the privacy notice and for uses and disclosures determined by the CHO to be compatible with those specified in the notice.¹⁰

Openness

- Must publish a privacy notice describing policies and practices for processing PPI and provide this notice to anyone upon request.
- Must post this notice on the CHO's website (if applicable) and post a sign at intake locations, etc., stating the availability of the privacy notice.
- Must state in the privacy notice that it can be amended, and that any amendments may effect uses of information collected before the amendment.
- CHOs receiving federal funding need to make reasonable accommodations for persons with disabilities and provide information in languages other than English that are common in the community.¹¹

Access and Correction

- Must generally allow a client to inspect and have copy of any PPI.

⁸ 69 Fed. Reg. 45929 (7-30-2004).

⁹ Id.

¹⁰ 69 Fed. Reg. 45930 (7-30-2004).

¹¹ Id.

- Must offer to explain information that the client doesn't understand.
- Must consider any request by a client to correct inaccurate or incomplete PPI.
 - A CHO may remove, supplement, or simply mark the PPI information inaccurate or incomplete as the circumstance may warrant.¹²

Accountability

- Must establish procedure for accepting and considering complaints about privacy and security policies and practices.
- Must require all staff members to sign a confidentiality agreement that acknowledges receipt of and pledging to comply with the privacy notice.¹³

This two-tiered approach towards HMIS data is designed to provide a uniform floor of protection for homeless clients with the possibility of additional protections for organizations with additional needs or capacities. A CHO's privacy policy is a critical factor for guiding the level of protection of client information. The baseline standards mentioned above seek to protect the confidentiality of personal information. These privacy and security standards are based on principles of fair information practices and on security standards recognized by the information privacy and technology communities. The standards were developed after review and consideration of the Health Insurance Portability and Accountability Act (HIPAA) standards for securing and protecting patient information. It is HUD's understanding that very few homeless providers are "covered entities" under HIPAA.¹⁴ When a homeless service provider is a covered entity, the provider is required to operate in accordance with HIPAA regulations. The final Notice in the Federal Register states that such a provider is not required to comply with the HMIS privacy or security standards because exempting HIPAA covered entities from the HMIS privacy and security rules avoids all possible conflicts between the two sets of rules.¹⁵ Thus, where a homeless service provider is not a covered entity under HIPAA, it is subject to the HMIS privacy and security standards.¹⁶ With this baseline requirement in perspective, what follows next is guidance on disclosures of HMIS data to law enforcement officials.

V. HUD's Guidance For Disclosures Of Information To Law Enforcement Officials

As mentioned above, in an effort to clarify disclosure provisions for law enforcement purposes, HUD describes in the July 30, 2004 Federal Register how it looked to HIPAA standards to clarify HMIS disclosure provisions:

The standards pertaining to the uses and disclosures of information were based on the standards set forth in HIPAA. The general principle in HIPAA is that a

¹² Id.

¹³ 69 Fed. Reg. 45931 (7-30-2004).

¹⁴ 69 Fed. Reg. 45895 (7-30-2004).

¹⁵ Id.

¹⁶ Id.

covered entity is permitted, but not required, to disclose protected health information for law enforcement purposes, without an individual's authorization, for six specified purposes or situations. HIPAA allows covered entities to disclose protected health information to a law enforcement official:

- (1) As required by law or in compliance with court orders, subpoenas, and administrative requests;
- (2) To identify or locate a suspect, fugitive, material witness, or missing person;
- (3) In response to a law enforcement official's request for information about a victim or suspected victim of a crime;
- (4) To alert law enforcement of a person's death, if the covered entity suspects that criminal activity caused the death;
- (5) When a covered entity believes that protected health information is evidence of a crime that occurred on its premises; or
- (6) By a covered health care provider in a medical emergency not occurring on its premises, when necessary to inform law enforcement about the commission and nature of a crime, the location of the crime or crime victims, and the perpetrator of the crime. HIPAA clearly allows disclosure of protected health information to law enforcement officials under several circumstances that do not involve court orders, warrants, or subpoenas.¹⁷

The July 30, 2004 Federal Register goes on to state HUD's position:

In accordance with HIPAA standards, the final Notice adopts the general principle that all uses and disclosures are permissive and not mandatory, except for first party access to records and any required disclosures for oversight of compliance with HMIS privacy and security standards. However, HUD recognizes the particularly sensitive circumstances within certain programs and has made the following modifications to the final Notice. Among the permitted disclosures to law enforcement, this final Notice specifies that service providers may (but are not required to) disclose protected information in response to a law enforcement official's oral request for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person. In this case, the protected information is limited to name, address, date of birth, place of birth, SSN, and distinguishing physical characteristics. This provision is comparable to HIPAA. Furthermore, service providers may (but are not required to) disclose protected information for other law enforcement purposes to a law enforcement official if the law enforcement official: Makes a written request that is signed by a supervisory official of the law enforcement agency seeking the protected information; states that the information is relevant and material to a legitimate law enforcement investigation; identifies the protected information sought; is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; and states that de-identified information could not be used to accomplish the purpose of the disclosure. This requirement is more restrictive than HIPAA.¹⁸

¹⁷ 69 Fed. Reg. 45896 (7-30-2004).

¹⁸ Id.

VI. When Does HIPAA Permit Disclosures To Law Enforcement Officials?

Since HUD was very much guided by HIPAA in determining when disclosures to law enforcement officials are appropriate, a review of the applicable HIPAA regulations is illuminating. Regarding public health information, a covered entity may disclose protected health information for a law enforcement purpose to a law enforcement official if the following applicable conditions are met:

(1) Pursuant to process and as otherwise required by law

A covered entity may disclose protected health information:

- As required by law including laws that require the reporting of certain types of wounds or other physical injuries; or
- In compliance with:
 - A court order or court-ordered warrant, or a subpoena or summons issued by a judicial officer;
 - A grand jury subpoena; or
 - An administrative request, including an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process authorized under law, provided that: (1) The information sought is relevant and material to a legitimate law enforcement inquiry; (2) The request is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; and (3) De-identified information could not reasonably be used.¹⁹

(2) Limited information for identification and location purposes

A covered entity may disclose protected health information in response to a law enforcement official's request for such information for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person, provided that:

- The covered entity may disclose only the following information:
 - Name and address;
 - Date and place of birth;
 - Social security number;
 - ABO blood type and rh factor;
 - Type of injury;
 - Date and time of treatment;
 - Date and time of death, if applicable; and
 - A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos.
- Except as permitted above the covered entity may not disclose for the purposes of identification or location any protected health information related to the individual's DNA or DNA analysis, dental records, or typing, samples or analysis of body fluids or tissue.²⁰

¹⁹ See: 45 CFR 164.512.

²⁰ Id.

(3) Victims of a crime

Except for disclosures required by law mentioned above, a covered entity may disclose protected health information in response to a law enforcement official's request for such information about an individual who is or is suspected to be a victim of a crime, if:

- The individual agrees to the disclosure; or
- The covered entity is unable to obtain the individual's agreement because of incapacity or other emergency circumstance, provided that
 - The law enforcement official represents that such information is needed to determine whether a violation of law by a person other than the victim has occurred, and such information is not intended to be used against the victim;
 - The law enforcement official represents that immediate law enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure; and
 - The disclosure is in the best interests of the individual as determined by the covered entity, in the exercise of professional judgment.²¹

(4) Decedents

A covered entity may disclose protected health information about an individual who has died to a law enforcement official for the purpose of alerting law enforcement of the death of the individual if the covered entity has a suspicion that such death may have resulted from criminal conduct.²²

(5) Crime on premises

A covered entity may disclose to a law enforcement official protected health information that the covered entity believes in good faith constitutes evidence of criminal conduct that occurred on the premises of the covered entity.²³

(6) Reporting crime in emergencies

A covered health care provider providing emergency health care in response to a medical emergency, other than such emergency on the premises of the covered health care provider, may disclose protected health information to a law enforcement official if such disclosure appears necessary to alert law enforcement to:

- The commission and nature of a crime;
- The location of such crime or of the victim(s) of such crime; and
- The identity, description, and location of the perpetrator of such crime.

²¹ Id.

²² Id.

²³ Id.

If a covered health care provider believes that the medical emergency is the result of abuse, neglect, or domestic violence of the individual in need of emergency health care, then the above does not apply and any disclosure to a law enforcement official for law enforcement purposes is subject to the “victims of a crime” section above.²⁴

VII. Several Examples Of What This Means To A Provider Organization

The following situations and examples attempt to illustrate when a covered homeless organization may disclose protected personal information to a law enforcement official:

Situation 1: In response to a lawful court order, court-ordered warrant, subpoena or summons issued by a judicial officer, or a grand jury subpoena.

Example 1:

The police arrive at the premises of a CHO with a legally sufficient search warrant authorizing the search and removal of records containing PPI. A CHO that allows the police to exercise the warrant does not violate the HMIS standard because a search warrant constitutes legal authority to seize records.²⁵

Situation 2: If the law enforcement official makes a written request for protected personal information that:

- (1) Is signed by a supervisory official of the law enforcement agency seeking the PPI;
- (2) States that the information is relevant and material to a legitimate law enforcement investigation;
- (3) Identifies the PPI sought;
- (4) Is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; and
- (5) States that de-identified information could not be used to accomplish the purpose of the disclosure.

Example 2:

A police officer brings a written request signed by a supervisory official asking for access to the CHO’s client database to browse through it for names the police may be interested in. The CHO refuses the request. The refusal is required by the standard because the request is not specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought and because the request does not state that de-identified information could not be used to accomplish the purpose of the disclosures.²⁶

²⁴ 45 CFR 164.512.

²⁵ See: U.S. Department of Housing and Urban Development: *Homeless Management Information System Data and Technical Standards Notice Frequently Asked Questions*. July 2005, p.11.

²⁶ Id.

Situation 3: If the CHO believes in good faith that the PPI constitutes evidence of criminal conduct that occurred on the premises of the CHO.

Example 3:

A client of a shelter assaults another client in the dining room of the shelter. The CHO calls the police and discloses the names of the individuals involved and the circumstances of the assault. The disclosure is consistent with the standard because the PPI disclosed is evidence of a crime that occurred on the premises of the CHO.²⁷

Situation 4: In response to an oral request for the purpose of identifying or locating a suspect, fugitive, material witness or missing person and the PPI disclosed consists only of name, address, date of birth, place of birth, Social Security Number, and distinguishing physical characteristics.

Example 4:

A local police officer asks a CHO for information to help in locating a suspect believed to be homeless. The CHO discloses information about the name, Social Security Number, and distinguishing physical characteristics of several clients. The disclosure is consistent with the standard.²⁸

Situation 5: If (1) the official is an authorized federal official seeking PPI for the provision of protective services to the President or to foreign heads of state or other persons authorized by federal law or for the conduct of investigations (such as threats against the President and others); and (2) The information requested is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought.

Example 5:

The local police ask a CHO to disclose information about the location of named homeless clients for use in connection with a Presidential visit planned in the next week. The CHO refuses to disclose the PPI. The refusal is permitted by the standard because disclosures made in connection with the provision of protective services must be to an authorized *federal* official.²⁹

Note that an organization must comply with all federal, state and local laws as the HUD privacy standards are the baseline. What follows next is more examples of the nexus between homeless service providers utilizing HMIS and law enforcement officials seeking information.

²⁷ Id.

²⁸ See: U.S. Department of Housing and Urban Development: *Homeless Management Information System Data and Technical Standards Notice Frequently Asked Questions*. July 2005, p.12.

²⁹ Id.

VIII. Other Disclosure Situations and Examples That Could Involve Law Enforcement Officials Disclosures

Uses and disclosures required by law

A CHO may use or disclose PPI when required by law. The HMIS baseline standard allows a CHO to disclose PPI if the disclosure complies with, and is limited to, the requirements of the law. That is, if a request for PPI is based on, and within the scope of, a specific legal requirement, the CHO may disclose the PPI without violating the HMIS standard. The law must *require* (and not merely permit) the disclosure. The example below demonstrates how this provision may be applied.

Example:

The local police ask for access to the CHO's client database to browse through it for names of persons the police are interested in locating. The police cite a section of the Patriot Act of 2001 as authority for the request. The CHO refuses to make the disclosure, and the refusal is consistent with and required by the HMIS privacy standard. The Patriot Act allows the Director of the Federal Bureau of Investigation to seek a court order requiring the production of books, records, papers, documents, and other items for an investigation to protect against international terrorism or clandestine intelligence activities. The authority of this section of the Patriot Act cannot be exercised either by local police or without a court order.³⁰

Uses and disclosures to avert a serious threat to health or safety

A CHO may use or disclose PPI if:

- (1) The CHO, in good faith, believes the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of an individual or the public; and
- (2) The use or disclosure is made to a person reasonably able to prevent or lessen the threat to health or safety.

Example:

The police ask a CHO for the name and other information about an individual believed to have left the CHO's homeless shelter and who is now holding another individual hostage. The CHO discloses the name and Social Security Number of the individual. It declines to provide other information in its possession because it does not believe that the additional information would be helpful in preventing or lessening the threat. The disclosure of the name is consistent with the standard. The refusal to disclose other information is also consistent with the standard.³¹

³⁰ See: U.S. Department of Housing and Urban Development: *Homeless Management Information System Data and Technical Standards Notice Frequently Asked Questions*. July 2005, p.9.

³¹ See: U.S. Department of Housing and Urban Development: *Homeless Management Information System Data and Technical Standards Notice Frequently Asked Questions*. July 2005, p.10.

Uses and disclosures about victims of abuse, neglect or domestic violence

A CHO may disclose PPI about an individual whom the CHO reasonably believes to be a victim of abuse, neglect or domestic violence to a government authority (including a social service or protective services agency) authorized by law to receive reports of abuse, neglect or domestic violence under any of the following circumstances:

- (1) Where the disclosure is required by and complies with the law;
- (2) If the individual agrees to the disclosure; or
- (3) To the extent that the disclosure is expressly authorized by statute or regulation and the CHO believes the disclosure is necessary to prevent serious harm to the individual or other potential victims or if the individual is unable to agree because of incapacity, a law enforcement or other public official authorized to receive the report represents that the PPI for which disclosure is sought is not intended to be used against the individual and that an immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.

A CHO that makes a permitted disclosure about victims of abuse, neglect or domestic violence must promptly inform the individual that a disclosure has been or will be made, except if: The CHO, in the exercise of professional judgment, believes informing the individual would place the individual at risk of serious harm or the CHO would be informing a personal representative (such as a family member or friend), and the CHO reasonably believes the personal representative is responsible for the abuse, neglect or other injury, and that informing the personal representative would not be in the best interests of the individual as determined by the CHO, in the exercise of professional judgment.

Example 1:

A CHO discloses PPI to a law enforcement agency with the oral consent of the victim. The disclosure is consistent with the standard.³²

Example 2:

The police ask for information about a victim of domestic violence under a specific statutory provision that authorizes disclosure of PPI to the police. The police orally assure the CHO that they do not intend to use the PPI against the victim. The police also represent that they have an immediate law enforcement need for the PPI that would be significantly affected by a delay to seek the consent of the individual. The CHO is unable to obtain consent because of the victim's incapacity. Because the statutory provision authorizes but does not require disclosure, the CHO declines to disclose the information, which is consistent with the standard. The CHO may choose to disclose the information, provided that the CHO informs the victim that the disclosure was made at the first opportunity.³³

³² Id.

³³ Id.

IX. Conclusion and Disclaimer

This memorandum offers information about the law but information is not the same as legal advice because of the nuances of the application of the law to specific circumstances and facts. HomeBase recommends you consult an attorney if you want professional assurance that information, the interpretation of it, and the application to a specific situation is appropriate. This memorandum is not intended as a substitute for getting a legal opinion on a specific matter. As noted in the beginning, matters concerning criminal investigations should always be examined on a case-by-case basis in order to best assess all parties' rights and duties. The purpose of this memorandum is to explain and educate, in a general way, the basics on search warrants, the various sources of authority on disclosing to law enforcement officials HMIS information, HUD's guidance on the issue as well as a offering a variety of situations and examples to assist in greater understanding of this complex matter.

For more information, please feel free to contact Michael Land, HomeBase Staff Lawyer, via email at Michael@homebaseccc.org, or by phone at 415.788.7961 x310.