The Network
for Public Health Law

Snap Shot

# Homeless Management Information Systems

**Federal Law:** Homeless Management Information Systems Privacy Standards

**Citation:** 42 U.S.C. § 11360a; 24 C.F.R. § 578.7; 24 C.F.R. § 578.57; 24 C.F.R. § 578.103; 69 FR 45888

HMIS seeks to protect the confidentiality of personal information.

## THE LAW

### What does the law do?

Homeless Management Information Systems (HMIS) are community-based systems to collect counts of individuals and families experiencing homelessness. HMIS are required by the Homeless Emergency Assistance and Rapid Transition to Housing (HEARTH) Act of 2009 and are used in the administration of several programs administered by the Department of Housing and Urban Development (HUD). The baseline privacy and security standards for HMIS (HMIS Privacy and Security Standards) are currently set by the Homeless Management Information Systems (HMIS); Data and Technical Standards Final Notice published in 2004. The HMIS Privacy and Security Standards "seek to protect the confidentiality of personal information while allowing for reasonable, responsible, and limited uses and disclosures of data."

### To whom does the law apply?

A Continuum of Care is responsible for designating an HMIS for its geographic area. Any homeless organization that "records, uses or processes protected personal information on homeless clients for an HMIS" is a covered homeless organization (CHO) and required to comply with the HMIS Privacy and Security Standards for HMIS administration.

## SHARING OF IDENTIFIABLE DATA

### How is "identifiable" information defined?

The HMIS Privacy and Security Standards define "Protected Personal Information" (PPI) as information maintained by or for a CHO about a living 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."

### Does this law allow identifiable data to be shared?

The HMIS Privacy and Security Standards permit four broad categories of PPI use or disclosure by CHOs: 1) service provision/coordination; 2) service payment/reimbursement; 3) administrative functions (e.g., audit, oversight); and 4) PPI de-identification. In addition to these four categories, a CHO can choose to use or disclose PPI for other specific uses or disclosures after "balancing the competing interests in a responsible and limited way." The other permissive uses and disclosure provisions are: 1) uses and disclosures required by law; 2) uses and disclosures in response to a serious threat to health or safety; 3) uses and disclosures about victims of abuse, neglect or domestic violence; 4) uses and disclosures for academic research purposes; and 5) uses and disclosures for law enforcement purposes. All other uses and disclosures not specified in the HMIS Privacy and Security Standards require the consent of the individual.

### Among who?

The HMIS Privacy and Security Standards do not specifically limit the entities or individuals that can receive PPI from HMIS. However, some of the disclosure exceptions do include some limitations. Disclosures to avert a serious health or safety threat must be made to someone reasonably able to prevent or lessen the threat. Disclosures about victims of abuse, neglect or domestic violence must be to an authorized government authority. Disclosures for academic research are limited to individuals or institutions with formal relationships with the CHO. Disclosures for law enforcement purposes are limited to law enforcement officials.

### What are the prerequisites and conditions?

The HMIS Privacy and Security Standards contain general conditions for HMIS data collection and use, including a requirement for CHOs to have a privacy notice that describes the purpose for PPI collection and all uses and disclosures. Additionally, CHOs must have accountability procedures, including a process for handling questions or complaints, requirements for CHO staff to comply with the CHO privacy notice, and confidentiality agreements. The HMIS must also comply with specific security standards.

There are specific requirements for each of the permissive disclosure provisions. For example, uses and disclosures for academic research require a written research agreement, and uses and disclosures to avert a threat to health or safety must be consistent with legal and ethical standards and require a good faith belief the use or disclosure is necessary to prevent or lessen a serious and imminent threat.

## SHARING OF DE-IDENTIFIED DATA

### Does this law allow de-identified information to be shared?

The HMIS Privacy and Security Standards only protect PPI, which is identifiable by definition. There are no specific limitations on sharing de-identified information.

### Does this law define de-identification or standards to render the data de-identified?

The HMIS Privacy and Security Standards do not specify a process to render PPI legally de-identified. The HMIS Privacy and Security Standards indicate that eight of the universal data elements are PPI (i.e., name, social security number, date of birth, zip code, program entry date, program exit date, unique personal identification number, program identification number). A 2006 HUD publication, Technical Guidelines for Unduplicating and De-identifying HMIS Client Records, proposed using the SHA-1 one-way hash message digest algorithm for de-identifying HMIS records.

## DATA SHARING IMPLICATIONS FOR PUBLIC HEALTH

### Does this law support data sharing to improve the health of communities?

Homelessness is a critical issue relating to community health. Accordingly, leveraging information about homeless individuals could help facilitate better public health interventions or efficient use of resources. The HMIS Privacy and Security Standards permit sharing data for a number of purposes that could promote community health, including disclosures required by law, disclosures to avert a threat to health or safety, disclosures about victims of abuse, neglect, or domestic violence, and disclosures for academic research.

## How does this law hinder data sharing to improve the health of communities?

The HMIS Privacy and Security Standards lack a provision permitting disclosures for public health purposes. The "required by law" disclosure provision needs specific legislative authority. The "threat to health or safety" disclosure provision requires a "serious and imminent" threat (a relatively high standard). The victim disclosure provision is tailored narrowly to issues relating abuse, neglect and domestic violence. The academic research provision is not suited for ongoing public health activities. Accordingly, it could be difficult to support an on-going public health activity given these limited disclosure provisions.

## Does this law establish prerequisites, conditions, or limitations for data sharing, not previously identified?

The HMIS Privacy and Security Standards provide "floor" protections that permit organizations and state and local governments to provide additional confidentiality protections.

## What other terms apply to sharing this data?

The HMIS Privacy and Security Standards do not apply to a CHO if it is covered entity under the Health Insurance Portability and Accountability Act (HIPAA) if "a substantial portion of its PPI" is protected health information as defined by HIPAA. The HEARTH Act requires HUD to promulgate regulations for HMIS; however, final regulations have not been promulgated as of 2017. Until then, HUD instructs its grantees to follow the HMIS Privacy and Security Standards.

## What remedies or solutions might be employed to support data sharing while complying with this law?

Homelessness is a significant social determinant of health with strong associations with many serious adverse health outcomes. Accordingly, there is a reasonable argument that homelessness poses a "serious and imminent threat to the health or safety" for homeless individuals. If an evidence-based intervention exists and requires the disclosure of HMIS data to lessen or prevent the threat to health or safety, then this provision could be used to support disclosure and use for the intervention.

## What ethical considerations apply to the exercise of discretion to share data under this law?

Homeless individuals are vulnerable populations that might feel coerced to provide private information to receive needed services. The HMIS Privacy and Security Standards state that individual consent to collect, use, and disclose information (consistent with the posted privacy policy) can be inferred in many circumstances. Consequently, not all individuals may fully appreciate the extent of permitted data uses and disclosures or might suffer from mental illness that interfere with their capacity to provide informed consent. Homeless individuals are sometimes stigmatized, so inappropriate disclosure of HMIS data could result in social harms.

Additional information on HMIS Regulations and guidance can be found here.

**SUPPORTERS**

**The Network for Public Health Law is a national initiative of the Robert Wood Johnson Foundation.**

**This document was developed by Cason Schmit, Research Assistant Professor, Texas A&M University and reviewed by Jennifer Bernstein, Deputy Director, Mid-States Region of The Network for Public Health Law. The Network for Public Health Law provides information and technical assistance on issues related to public health. The legal information and assistance provided in this document does not constitute legal advice or legal representation. For legal advice, please consult specific legal counsel.**

**October, 2018**