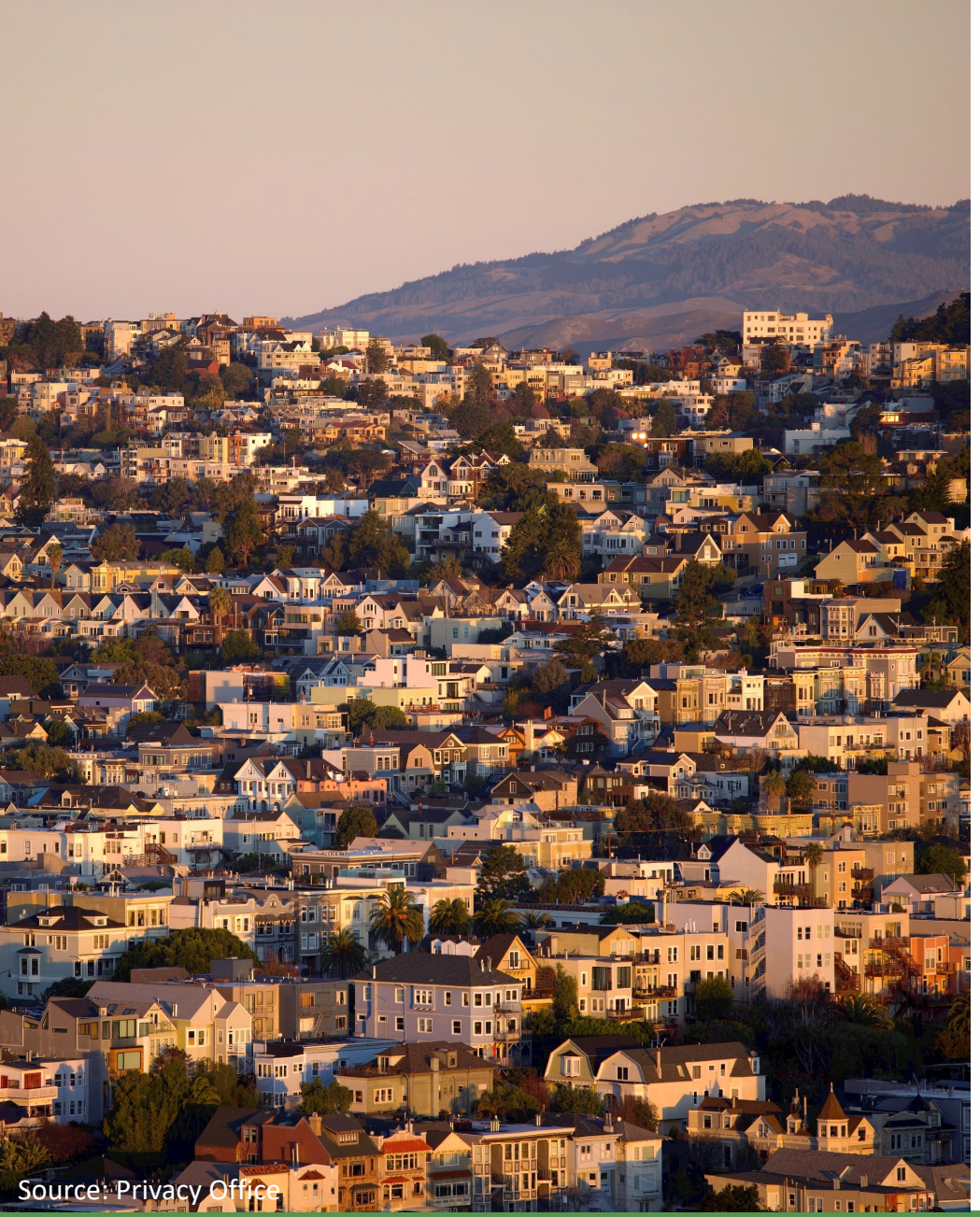
DEPARTMENT OF HOMELESSNESS AND SUPPORTIVE HOUSING

Allowable Uses and Disclosures of Personal Information

Local Homeless Coordinating Board Meeting

July 7, 2025


Source: Privacy Office

What is Personal Identifiable Information (PII)?

Personal Identifiable Information (PII)

- Homeless Management Information System (HMIS) Privacy Standards define Protected Personal Information (i.e., Personal Identifiable Information or PII) as any information maintained by a Covered Homeless Organization* about a living homeless client or homeless individual that:

    1. Identifies, directly or indirectly, a specific individual;

    2. Can be manipulated by a reasonably foreseeable method to identify an individual; or

    3. Can be linked with other available information to identify a specific individual.

* Any organization (including its employees, volunteers, affiliates, contractors, and associates) that records, uses or processes PPI on homeless clients for an HMIS.

Examples of PII

NIST Examples of PII			
Age	Email addresses	Investigation report or database	Race/ethnicity
Alias	Employee identification number	IP/MAC address	Religion
Audio recordings	Employment status, history, or information (e.g., title, position)	Legal documents or records	Salary
Biometric identifiers, (e.g., fingerprints, iris image)	Fax number	Marital status	Sex
Certificates (e.g., birth, death, marriage)	Financial information	Military status or other information	Social Security number (SSN)
Credit card number	Foreign activities	Mother's maiden name	Taxpayer ID
Criminal records information	Full name	Passport information	User ID
Date of birth	Gender	Phone numbers	Vehicle identifiers
Device identifiers (e.g., mobile devices)	Geolocation information	Photographic identifiers	Web uniform resource locators
Driver's license/state ID number	Home address	Place of birth	Work address or other business contact information
Educational records	Internet cookies containing PII	Protected health information	

Source: National Institute of Standards and Technology (NIST) Special Publication (SP) 800-122, "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)."

Common Examples of PII in HMIS

NIST Examples of PII			
Age	Email addresses	Investigation report or database	Race/ethnicity
Alias	Employee identification number	IP/MAC address	Religion
Audio recordings	Employment status, history, or information (e.g., title, position)	Legal documents or records	Salary
Biometric identifiers, (e.g., fingerprints, iris image)	Fax number	Marital status	Sex
Certificates (e.g., birth, death, marriage)	Financial information	Military status or other information	Social Security number (SSN)
Credit card number	Foreign activities	Mother's maiden name	Taxpayer ID
Criminal records information	Full name	Passport information	User ID
Date of birth	Gender	Phone numbers	Vehicle identifiers
Device identifiers (e.g., mobile devices)	Geolocation information	Photographic identifiers	Web uniform resource locators
Driver's license/state ID number	Home address	Place of birth	Work address or other business contact information
Educational records	Internet cookies containing PII	Protected health information	

Source: National Institute of Standards and Technology (NIST) Special Publication (SP) 800-122, "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)."

Source: Privacy Office

How does HSH use and disclose PII?

HMIS Uses and Disclosures

- HMIS Privacy Standards allow HSH and its partners to use or disclose PII under the following circumstances:

1. To provide or coordinate services to an individual;

2. For functions related to payment or reimbursement of services;

3. To carry out administrative functions, including but not limited to legal, audit, personnel, oversight and management functions; or

4. For creating de-identified PII.

Additional Uses and Disclosures

- To strike a balance between organizations' competing interests and obligations in "a responsible and limited way," HMIS Privacy Standards and the HSH Privacy Notice permit additional uses and disclosures of PII under certain conditions, including:
  - Uses and disclosures required by law;
  - Uses and disclosures to avert a serious threat to health or safety;
  - Uses and disclosures about victims of abuse, neglect or domestic violence;
  - Uses and disclosures for academic research purposes; and
  - Disclosures for law enforcement purposes.

Disclosures for Law Enforcement Purposes

- HSH may disclose PII for law enforcement purpose under the following circumstances:
  - In response to a lawful court order, subpoena or summons;
  - In response to a written request for information (under limited conditions);
  - In response to an oral request for the purpose of identifying or locating a suspect, fugitive, material witness or missing person;
  - If HSH believes in good faith that the PII constitutes evidence of criminal conduct that occurred on its premises; or
  - If the requestor is an authorized federal official seeking PII for the provision of protective services to the President or a foreign head of state.

Disclosure Must Be Authorized

- Disclosure must be consistent with HMIS Privacy Standards and the HSH Privacy Notice. HSH will never disclose PII without confirming the authenticity and legality of a request.

- Recent requests submitted to HSH that, if granted, may have resulted in unlawful disclosure include:

  - A request included in an invalid subpoena
  - A request from a person seeking information about in client in their neighborhood
  - A request from a person in a different country claiming to be a friend of a client
  - A Sunshine request for “an export of the entire ONE System database”

Sanctuary City Ordinance

- San Francisco Administrative Code Chapter 12H (Sanctuary City Ordinance) prohibits HSH from using City funds or resources to assist federal agencies, including Immigration and Customs Enforcement (ICE), with the arrest and/or gathering or dissemination of information regarding the release status or the personal or confidential information of an individual, unless it is mandated by federal or state law, warrant, or court decision.

- If it were to receive a request for PII for the purpose of immigration enforcement activities, the Privacy Office will immediately notify HSH Leadership and coordinate with the City Attorney's Office on its response to the request.

- Partner agencies are required to notify the HSH Privacy Office of all legal requests for PII.

- HSH and its partners do not collect PII on citizenship, legal status, or country of origin.

Privacy is Everyone's Responsibility

- HMIS System Administrator (Bitfocus): HMIS data is confidential and the sole property of the HMIS Lead Agency. System Administrator provides data access privileges solely for the purpose of providing or coordinating services.

- HMIS Lead Agency: HSH manages all access to HMIS and oversees all privacy, security, and compliance policies and procedures.

- HSH Partner Agencies: Partner agencies and their respective end users are responsible for complying with all privacy, security, and compliance obligations, including contracts and data sharing agreements, HMIS Participation Agreements, the DPH Code of Conduct, confidentiality attestations, etc. Partner agencies and end users are subject to monitoring and auditing by HSH.

Source: Privacy Office

Questions?