

Policy Title:	De-identification of Client Information and Use of Limited Data Sets			
Policy Number:	DHS-100-007	Version:	2.0	Effective Date: Upon Approval

Signature on File in the office of the Chief Administrative Officer

Approved: Jeremy Emerson, Interim CAO

Date: July 20, 2009

Overview

Purpose/Rationale:

The intent of this policy is to prescribe standards under which client information can be used and disclosed if information that can identify a person has been removed or restricted to a limited data set.

Policy

1. General

- a. De-identified information is client information from which DHS or another entity has deleted, redacted, or blocked identifiers, so that the remaining information cannot reasonably be used to identify a person.
- b. Unless otherwise restricted or prohibited by other federal or state law, DHS can use and disclose information as appropriate for the work of DHS, without further restriction, if DHS or another entity has taken steps to de-identify the information consistent with the requirements and restrictions of this policy in Section (2.).
- c. DHS may use or disclose a limited data set that meets the requirements of Section (4.) of this Policy, if DHS enters into a data use agreement with the limited data set recipient (or with the data source, if DHS will be the recipient of the limited data set) in accordance with the requirements of Section (5.) of this Policy.
- d. DHS may disclose a limited data set only for the purposes of research, program operations, or public health purposes. However, unless DHS has obtained a limited data set that is subject to a data use agreement, DHS is not restricted to using a limited data set for its own activities or operations.
- e. If DHS knows of a pattern or activity or practice of the limited data set recipient that constitutes a material breach or violation of a data set agreement, DHS will take reasonable steps to cure the breach or end the violation. If such steps are unsuccessful, DHS will discontinue disclosure of information to the recipient and report the problem to the U.S. Department of Health and Human Services, Office for Civil Rights.

2. Requirements for de-identification of client information

- a. DHS may determine that client information is sufficiently de-identified, and cannot be used to identify an individual, only if **either** (A.) or (B.) below have occurred:
 - A. A statistician or other person with appropriate knowledge of, and experience with, generally accepted statistical and scientific principles and methods for rendering information not individually identifiable:
 - i. Has applied such principles and methods, and determined that the risk is minimal that the information could be used, alone or in combination with other reasonably available information, by a recipient of the information to identify the person whose information is being used; and
 - ii. Has documented the methods and results of the analysis that justify such a determination; **or**
 - B. DHS has ensured that:
 - i. The following identifiers of the individual or of relatives, employers, and household members of the individual are removed:
 - I. Names;
 - II. All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geo codes. However, the initial three digits of a zip code may remain on the information if, according to current publicly-available data from the Bureau of the Census, the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and the initial three digits for all such geographic unit containing 20,000 or fewer people is changed to 000;
 - III. All elements of dates (except year) for dates directly relating to an individual, including birth date, dates of admission and discharge from a health care facility, and date of death. For persons age 90 and older, all elements of dates (including year) that would indicate such age must be removed, except that such ages and elements may be aggregated into a single category of "age 90 or older;"
 - IV. Telephone numbers;
 - V. Fax numbers;
 - VI. Electronic mail addresses;
 - VII. Social security numbers;
 - VIII. Medical record numbers;
 - IX. Health plan beneficiary numbers;

- X. Account numbers;
- XI. Certificate or license numbers;
- XII. Vehicle identifiers and serial numbers, including license plate numbers;
- XIII. Device identifiers and serial numbers;
- XIV. Web Universal Resource Locators (URLs);
- XV. Internet Protocol (IP) address numbers;
- XVI. Biometric identifiers, including fingerprints and voiceprints;
- XVII. Full face photographic images and any comparable images; and
- XVIII. Any other unique identifying number, characteristic, or codes, except as permitted under Section (3.) of this policy; **and**
 - ii. DHS has no actual knowledge that the information could be used alone or in combination with other information to identify an individual who is the subject of the information.

3. Re-identification of de-identified information

- a. DHS may assign a code or other means of record identification to allow information de-identified under this policy to be re-identified by DHS, except that:
 - A. The code or other means of record identification is not derived from or related to information about the individual and cannot otherwise be translated to identify the individual; and
 - B. DHS does not use or disclose the code or other means of record identification for any other purpose, and does not disclose the mechanism for re-identification.

4. Requirements for a limited data set

- a. A limited data set is information that excludes the following direct identifiers of the individual, or of relatives, employers or household members of the individual:
 - A. Names;
 - B. Postal address information, other than town or city, State and zip code;
 - C. Telephone numbers;
 - D. Fax numbers;
 - E. Electronic mail addresses;
 - F. Social Security numbers;

- G. Medical record numbers;
- H. Health plan beneficiary numbers (such as Medicaid Prime Numbers);
- I. Account numbers;
- J. Certificate/license numbers;
- K. Vehicle identifiers and serial numbers, including license plate numbers;
- L. Web Universal Resource Locators (URLs);
- M. Internet Protocol (IP) address numbers;
- N. Biometric identifiers, including finger and voice prints; and
- O. Full face photographic images and any comparable images.

5. Contents of a data use agreement

- a. DHS may disclose a limited data set only if the use of the data is permitted under applicable state or federal law and the entity receiving the limited data set enters into a written agreement with DHS, in accordance with subsection (5.) (b.) that such entity will use or disclose the protected health information only as specified in a written agreement.

Example: Information about applicants for and recipients of public assistance may only be used for purpose directly related to the administration of the public assistance programs, so disclosure of partially identifiable information (a limited data set) under a data use agreement must be limited to authorized purposes.

- b. A data use agreement between DHS and the recipient of the limited data set must:
 - A. Specify the permitted uses and disclosures of such information that will be made by the limited data set recipient. DHS may not use the agreement to authorize the limited data set recipient to use or further disclose the information in a manner that would violate the requirements of this Policy, **DHS Policy DHS-100-003 "Uses and Disclosures of Client or Participant Information"** or **DHS Policy DHS-100-002 "Client Privacy Rights"** if done by DHS.
 - B. Specify who is permitted to use or receive the limited data set; and
 - C. Specify that the limited data set recipient will:
 - i. Not use or further disclose the information other than as specified in the data use agreement or as otherwise required by law;
 - ii. Use appropriate safeguards to prevent use or disclosure of the information other than as specified in the data use agreement;

- iii. Report to DHS, if DHS is the source of the limited data set, if the recipient becomes aware of any use or disclosure of the information not specified in its data use agreement with DHS;
- iv. Ensure that any agents, including a subcontractor, to whom it provides the limited data set agrees to the same restrictions and conditions that apply to the limited data set recipient with respect to such information; and
- v. Not identify the information or contact the individuals whose data is being disclosed.

References

- 45 CFR 164.514
- [Privacy/Security Glossary of Common Terms](#)

Policy(ies) that apply:

[DHS-100-002](#) Client Privacy Rights

[DHS-100-003](#) Uses and Disclosures of Client or Participant Information

Contact(s):

- Jane Alm, DHS Privacy Officer, jane.alm@state.or.us
- Privacy Program Office, (503) 945-5780

Policy History:

- **Version 2.0:**
07/01/09: This policy originated in March 2003 in order to meet compliance with the federal HIPAA Privacy Rule. The 2009 revisions do not impact the policy's compliance with HIPAA. The revisions are implemented to improve clarity and to bring some of the language in line with other more familiar program-specific privacy language.
- **Version 1.0:**
03/31/2003: Initial Release