Operational Policy

Policy title:	**De-identification of Individual Information and Use of Limited Data Sets**		
Policy number:	DHS|OHA-100-011		
Original date:	7/22/2014 (OHA only)	**Last update:**	10/03/2016 (Joint DHS|OHA)
Approved:	Dr. Richardson, Deputy Director DHS Mark Fairbanks, OHA CFO		

Purpose

This policy is one of two that outline the Department of Human Services (DHS) and Oregon Health Authority (OHA) guidelines and expectations for protecting the privacy of information and maintaining reasonable safeguards when disclosing protected information.

Description

This policy describes the requirements for de-identification and re-identification and aggregation of identifiable or protected information and the requirements for creating, using and disclosing limited data sets. All staff should review their agencies privacy policies to be sure they understand how these policies work together to protect individual privacy.

Applicability

This policy applies to all DHS and OHA staff including employees, volunteers, trainees and interns.

As keepers of the public trust, all agency employees have a responsibility to comply with state and agency policies, administrative rule, and state and federal law. The agency takes this responsibility seriously and failure to fulfill this responsibility is not treated lightly. Employees who fail to comply with state or agency policy, administrative rule, or state and federal law may face progressive discipline, up to and including dismissal from state service.

Policy

1. Research means a systematic investigation, including research development, investigation, testing, and evaluation designed to develop or contribute to generalized knowledge.
2. Unless federal or state statute or rule otherwise restricts or prohibits the release of information, DHS and OHA may use and disclose data in order to accomplish the work of the agencies, including for research, public health or health care operations functions, if:
   a. The information has been sufficiently de-identified as required by this policy; and
   b. DHS and OHA have no actual knowledge that the data could be used alone or in combination with other available information to identify an individual who is a subject of the data.
3. De-identified data is created when information is removed from a data set by deleting, redacting or blocking the information so that the remaining information cannot reasonably be used to identify a specific individual.
4. De-identified information is not protected health information.

5. DHS or OHA may determine that individually identifiable information is sufficiently de-identified if a statistician or other person with knowledge of, and experience with, generally accepted statistical and scientific principles and methods for rendering information not individually identifiable:
   a. Has applied such principles and methods and determined that the risk is minimal that the data could be used, alone or in combination with other reasonably available information, to identify the individual who is the subject of the data; and
   b. Has documented the methods and results of the analysis that justify such a determination.
6. Instead of the method outlined in item five of this policy, DHS and OHA may use the form of de-identification, known as “Safe Harbor” as defined by the Federal Guidelines for De-identification of Protected Health Information.
7. A limited data set differs from a de-identified data set because it includes most dates and some geographic indicators. DHS or OHA may release a limited data set if a data use agreement is put in place and if the following specific identifiers of the individual and the individual’s relatives, employers, and household members are removed:
   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
   i. Account numbers
   j. Certificate or license numbers
   k. Vehicle identifiers and serial numbers, including license plate numbers
   l. Device identifiers and serial numbers
   m. Web Universal Resource Locators (URLs)
   n. Internet Protocol (IP) address numbers
   o. Biometric identifiers, including fingerprints and voiceprints
   p. Full face photographic images and any comparable images.
8. In addition to the above identifiers that must be removed to create a limited data-set, the below must be excluded if the use or disclosure of health information is to be considered completely de-identified, thus removing the data use agreement requirement:
   a. For persons under the age of 90, all date elements except year for any date directly relating to the individual, including birth date, dates of admission and discharge from a health care facility, and date of death.
   b. For persons age 90 and older, all date elements including year that would indicate age, except that such ages and elements may be aggregated into a single category identified as “age 90 or older”.
   c. All geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code, and equivalent geographic codes, except as otherwise described in item 9 of this policy.
   d. Any other unique identifying number, characteristic, or code, unless otherwise permitted by this policy.
   e. For persons under the age of 90, all date elements except year for any date directly relating to the individual, including birth date, dates of admission and discharge from a health care facility, and date of death.
   f. For persons age 90 and older, all date elements including year that would indicate age, except that such ages and elements may be aggregated into a single category identified as “age 90 or older”.

9. The initial three digits of a zip code need not be removed when the agencies are creating sufficiently de-identified information for use or release if:
    a. Current publicly available data from the Bureau of the Census confirms that the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and
    b. The initial three digits for geographic units containing 20,000 or fewer people is changed to 000.
10. DHS and OHA shall follow the minimum necessary standard required by federal statute and rule and agency policy when disclosing limited data sets to other authorized entities.
11. DHS or OHA may use or disclose a code or other record identifier assigned by the agency to permit the re-identification of de-identified data if:
    a. The code or record identifier is not derived from or related to information about the individual and cannot otherwise be used to identify the individual;
    b. DHS|OHA does not use or disclose the code or record identifier for any other purpose; and
    c. DHS|OHA does not disclose the mechanism for re-identification.
12. DHS or OHA may enter into data use agreements to obtain, use or disclose a limited data set as specified by the data use agreement, only if the use of the data is:
    a. Allowed under state or federal statute or rule.
    b. For research, program operations, or public health purposes.
13. Unless otherwise allowed or required by law, DHS and OHA shall not release limited data sets without receiving a data use agreement.
14. Unless DHS and OHA obtains data subject to a data use agreement, the agencies are not restricted to using limited data sets for their own activities or operations.
15. A data use agreement between DHS or OHA and the recipient of a limited data set shall include information related to:
    a. The identity of the recipient(s) who shall be permitted to obtain or use the limited data set.
    b. The allowed uses and disclosures of the data by the recipient.
    c. Assurances that the recipient will not use or disclose the information other than as specified in the data use agreement or as otherwise required by law.
    d. The use of appropriate safeguards to prevent use or disclosure of the information other than as specified in the data use agreement.
    e. Requirements for reporting to the agency if the recipient becomes aware of any use or disclosure of the information not specified in its data use agreement.
    f. Ensuring that any agents of the recipient agree to the same restrictions and conditions that apply to the recipient with respect to the limited data set.
    g. Confirmation that the recipient and the recipient's agents agree to not identify the information or contact the individuals whose data is being disclosed.
16. DHS and OHA may not use a data use agreement to authorize a limited data set recipient to use or further disclose information in a way that would violate the requirements of HIPAA or DHS|OHA policy related to an individual's privacy rights and the use and disclosure of individually identifiable information.
17. If DHS or OHA determines that the recipient of a limited data set has engaged in an activity or practice that constitutes a material breach or violation of the data use agreement, the agency shall take reasonable steps to ensure the breach is cured or the violation is ended.
18. If DHS or OHA determines that the recipient of a limited data set has engaged in an activity or practice that constitutes a material breach or violation of the data use agreement and efforts to cure the breach or violation are unsuccessful, the agency will discontinue disclosure of information and report the problem to the U.S. Department of Health and Human Services, Office for Civil Rights.
19. If DHS or OHA determine that aggregate data is identifiable, the agency shall mask or redact data sets containing small numbers prior to release.

a. Aggregated data is information tracked across time, organizations, individual populations or some other potentially identifiable variable.
b. Aggregate data replaces group observations with summary statistics of those observations including counts, percentages, averages or other statistical metrics.
c. Aggregate data does not include data on any single observation, family, individual, relative, employer, or household member of an individual.

20. If this policy conflicts with federal or state statute or rule that statute or rule supersedes unless this policy provides more protection.
21. DHS and OHA follow all applicable federal and state statutes and rules and all applicable Oregon Department of Administrative Services statewide policies.

References

OAR 409-021-0140
OAR 943-014-0420
45 CFR 164.514
45 CFR 164.502
Federal Guidelines for De-identification of Protected Health Information
Privacy/Security Glossary of Common Terms

Related policies

OHA Privacy Policies 100-001 to 100-014
DHS Privacy Policies

Contact

Information Security and Privacy Office (ISPO)
Phone: 503-945-6812 (Security)
503-945-5780 (Privacy)
Fax: 503-947-5396
Email: dhsinfo.security@state.or.us
dhs.privacyhelp@state.or.us

U. S. Department of Health and Human Services, Office for Civil Rights
Medical Privacy, Complaint Division
200 Independence Avenue, SW
Washington, D.C. 20201
Toll free Phone: 877-696-6775
Phone: 866-627-7748
TTY: 886-788-4989
Email: OCRComplaint@hhs.gov

Policy history

Version 1 OHA 100-011 established 7/22/2014
Version 1 DHS|OHA 100-011 established 10/03/2016

Keywords
IIndividual privacy, Notice of Privacy Practices, NPP, Protecting privacy, Release of information, Protected health information, PHI, Protected individual information, PII, Authorization, Release, Releasing information, Disclose, Disclosure, Access, Inspect, Personal representative, Data, De-identified data, Institutional Review Board, IRB Executor, Data sets, Data agreement, Data use

---

This document can be provided upon request in an alternate format for individuals with disabilities or in a language other than English for people with limited English skills. To request this document in another format or language, contact the Publications and Design Section at 503-378-3486, 7-1-1 for TTY, or email dhs-oha.publicationrequest@state.or.us.