

Policy Title:	General Privacy				
Policy Number:	DHS-100-001	Version:	2.0	Effective Date:	Upon Approval

Signature on File in the office of the Chief Administrative Officer

Approved by: Jeremy Emerson, Interim CAO

Date: July 20, 2009

Overview

Purpose/Rationale:

The intent of this policy is to outline DHS general guidelines and expectations for the necessary collection, use, and disclosure of confidential information about individuals in order to provide services and benefits to individuals, while maintaining reasonable safeguards to protect the privacy of their information.

Policy

1. General – DHS will safeguard confidential information about Individuals

- a. DHS may collect, maintain, use, transmit, share and/or disclose information about individuals to the extent needed to administer DHS programs, services and activities, consistent with federal and state confidentiality requirements applicable to the program, service or activity.
- b. DHS will safeguard all confidential information about individuals, inform individuals about DHS' privacy practices and respect individual privacy rights, to the full extent required under this policy.
- c. This policy identifies three types of individuals of whom DHS is most likely to obtain, collect or maintain individual information:
 - A. DHS Clients;
 - B. Participants; and
 - C. Licensees or Providers.
- d. DHS shall provide training to all employees on DHS' privacy policies, outlining their role and responsibilities relating to protecting the privacy of DHS clients and participants.

2. **Safeguarding information about Clients**

A "Client" is an individual who requests or receives services from DHS or through DHS contracted service providers.

- a. DHS, its employees, and business associates will respect and protect the privacy of records and information about clients who request or receive services from DHS. This includes, but is not limited to:
 - A. Applicants or recipients of public assistance;
 - B. Minors and adults receiving protective services from DHS;
 - C. Persons who apply for or are admitted to a state training center, a state-operated group home, a state hospital, or who are committed to the custody of DHS; and
 - D. Children in the custody of DHS either on a voluntary or committed basis.
- b. All DHS client information is confidential and must be safeguarded in accordance with DHS privacy policies and procedures.
- c. DHS shall not use or disclose information unless either:
 - A. The client has authorized the use or disclosure in accordance with **DHS Policy DHS-100-003**, "Uses and Disclosures of Client or Participant Information;" or
 - B. The use or disclosure is specifically permitted under **DHS Policy DHS-100-003**, "Uses and Disclosures of Client or Participant Information."
- d. DHS program offices shall adopt procedures to reasonably safeguard client information.

3. **Safeguarding information about Participants**

"Participants" are individuals participating in DHS population-based services, programs, and activities that serve the general population, but who do not receive program benefits or direct services that are received by a "client."

- a. When DHS or its business associates obtain individually identifiable information about participants, DHS may use and disclose such information consistent with Federal or State rules and regulations or DHS policies and procedures.
- b. DHS will safeguard all confidential information about participants consistent with Federal or State rules and regulations or DHS policies and procedures.

4. **Safeguarding information about Licensees and Providers**

A "Licensee" is a person or entity that applies for or receives a license, certificate, registration or similar authority from DHS to perform or conduct a service, activity or

function.

A "Provider" is a person or entity who may seek reimbursement from DHS as a provider of services to DHS clients.

- a. When DHS obtains information about licensees or providers, DHS may use and disclose such information consistent with Federal and State law and regulation. Information regarding the qualifications of licensees and providers are public records.
 - A. DHS will safeguard confidential information about licensees and providers consistent with Federal and State rules and regulations and DHS policies and procedures.
 - B. When DHS obtains information about individuals that relates to determining payment responsibility when a provider submits a claim or other request for payment to DHS, DHS will safeguard such information consistent with federal and state law and regulations and DHS policies and procedures.
 - C. DHS is also authorized to review the performance of licensees and providers in the conduct of their health oversight and other review activities.
 - D. DHS will safeguard confidential information about individuals obtained during health oversight and other review activities consistent with federal and state law and regulations and DHS policies and procedures.

5. Conflict with other requirements regarding privacy and safeguarding

- a. DHS has adopted reasonable policies and procedures for administration of its programs, services and activities. If any state or federal law or regulation, or order of a court having appropriate jurisdiction, imposes a stricter requirement upon DHS regarding the privacy or safeguarding of information, DHS shall act in accordance with that stricter standard.
- b. DHS staff shall act in accordance with established DHS policy and procedures regarding the safeguarding and confidentiality of individual information, whether health-related or not, in all DHS programs, services and activities.
- c. In the event that more than one policy applies but compliance with all such policies cannot reasonably be achieved, the DHS employee will seek guidance from supervisors according to established DHS policy and procedures. DHS staff should consult with their privacy coordinator or the DHS Privacy Program in the Information Security Office in appropriate circumstances.

6. DHS Notice of Privacy Practices.

- a. DHS will make available to each client a notice of DHS privacy practices that describes the responsibility of DHS to maintain the privacy of protected information and includes

a description that clearly informs the client of the types of uses and disclosures DHS is permitted or required to make.

- b. The DHS notice of privacy practices shall contain all information required under federal regulations regarding the notice of privacy practices for protected health information under HIPAA.
- c. DHS will provide all clients in direct care settings a notice of DHS privacy practices and will request the client's signature on an acknowledgement of receipt form.

7. Client Privacy Rights

DHS policies and procedures, as well as other federal and state laws and regulations, outline the client's right to access their own information, with some exceptions. This policy also describes specific actions that a client can take to request restrictions or amendments to their information, and the method for filing complaints. These specific actions are outlined in **DHS Policy DHS-100-002**, "Client Privacy Rights."

8. Uses and Disclosures of Client or Participant Information

DHS will not use or disclose any information about a client or participant of DHS programs or services without a signed authorization for release of that information from the individual, or the individual's personal representative, *unless* authorized by this policy and as otherwise allowed or required by state or federal law, as outlined in **DHS Policy DHS-100-003**, "Uses and Disclosures of Client or Participant Information."

9. Minimum Necessary Information

- a. DHS will use or disclose only the minimum amount of information necessary to provide services and benefits to clients, and only to the extent provided in DHS policies and procedures.
- b. This policy does not apply to:
 - A. Disclosures to or requests by a health care provider for treatment;
 - B. Uses or disclosures made to the individual;
 - C. Uses or disclosures authorized by the individual;
 - D. Disclosures made to the Secretary of the United States Department of Health and Human Services in accordance with federal HIPAA regulations at 45 CFR 160, Subpart C.
 - E. Uses or disclosures that are required by law; and

- F. Uses or disclosures required for compliance with federal HIPAA regulations at 45 CFR, Parts 160 and 164.
- C. When using or disclosing an individual's information, or when requesting an individual's information from a provider or health plan, DHS employees must make reasonable efforts to limit the amount of information to the minimum necessary needed to accomplish the intended purpose of the use, disclosure, or request, as outlined in **DHS Policy DHS-100-004**, "Minimum Necessary Information."

10. Administrative, Technical and Physical Safeguards

DHS staff must take reasonable steps to safeguard confidential information from any intentional or unintentional use or disclosure, as outlined in **DHS Policy DHS-100-005**, "Administrative, Technical, and Physical Safeguards."

11. Uses and Disclosures for Research Purposes and Waivers

DHS may use or disclose an individual's information for research purposes as outlined in **DHS Policy DHS-100-006**, "Uses and Disclosures for Research Purposes and Waivers." This policy specifies requirements for using or disclosing information with and without an individual's authorization, and identifies some allowable uses and disclosure of information when DHS is acting as a Public Health Authority.

12. De-Identification of Client Information and Use of Limited Data Sets

Unless otherwise restricted or prohibited by other federal or state law, DHS can use and share information as appropriate for the work of DHS, without further restriction, if DHS or another entity has taken steps to de-identify the information as outlined in **DHS Policy DHS-100-007**, "De-identification of Client Information and Use of Limited Data Sets."

13. Business Associate Relationships

DHS may disclose protected health information to business associates with whom there is a written contract or memorandum of understanding as outlined in **DHS Policy DHS-100-008**, "DHS Business Associate Relationships."

14. Enforcement, Sanctions and Penalties for Violations of Individual Privacy

All employees, volunteers, interns and members of the DHS workforce must guard against improper uses or disclosures of DHS client or participant's information as outlined in **DHS Policy DHS-100-009**, "Enforcement, Sanctions, and Penalties for Violations of Individual Privacy."

Forms that apply

- [DHS 2090](#), "DHS Notice of Privacy Practices"
- [DHS 2092](#), "DHS Notice of Privacy Practices, Acknowledgement of Receipt"

References

- 45 CFR Parts 160 and 164
- Privacy/Security Glossary of Common Terms
<http://www.dhs.state.or.us/policy/admin/security/glossary.htm>

Policy(ies) that apply:

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

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

[DHS-100-004](#) Minimum Necessary Information

[DHS-100-005](#) Administrative, Technical, and Physical Safeguards

[DHS-100-006](#) Uses and Disclosures for Research Purposes & Waivers

[DHS-100-007](#) De-identification of Client Information and Use of Limited Data Sets

[DHS-100-008](#) DHS Business Associate Relationships

[DHS-100-009](#) Enforcement, Sanctions, and Penalties for Violations of Individual Privacy

Contacts

- 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