

Policy Title:	Enforcement, Sanctions, and Penalties for Violations of Individual Privacy			
Policy Number:	DHS-100-009	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 specify enforcement, sanction, penalty, and disciplinary actions that may result from violation of DHS policies regarding the privacy and protection of an individual's information and to offer guidelines on how to conform to the required standards.

Policy

1. General

- a. All employees, volunteers, interns and members of the DHS workforce must guard against improper uses or disclosures of a DHS client or participant's information.
 - A. DHS employees, volunteers, interns and members of the DHS workforce who are uncertain if a disclosure is permitted are advised to consult with a supervisor in the DHS workplace.
 - B. The DHS Privacy Officer is a resource for any DHS workplace that cannot resolve a disclosure question, and may be consulted in accordance with the operational procedures of that DHS workplace.
- b. All employees are required to be aware of their responsibilities under DHS privacy policies.
- c. Supervisors are responsible for assuring that employees who have access to confidential information, whether it be electronic, hard copy, or orally, are informed of their responsibilities.
- d. DHS employees who violate DHS policies and procedures regarding the safeguarding of an individual's information are subject to disciplinary action by DHS up to and including immediate dismissal from employment, and legal action by the individual.
- e. DHS employees who knowingly and willfully violate state or federal law for improper use or disclosure of an individual's information are subject to criminal investigation and prosecution or civil monetary penalties.

- f. If DHS fails to enforce privacy safeguards, DHS as a state agency may be subject to administrative penalties by the U.S. Department of Health and Human Services, including federal funding penalties.

2. Retaliation prohibited

- a. Neither DHS as an entity nor any DHS employee will intimidate, threaten, coerce, discriminate against, or take any other form of retaliatory action against any individual or other person for:
 - A. Filing a complaint with DHS or with the U.S. Department of Health and Human Services as provided in DHS privacy policies;
 - B. Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing relating to DHS policy and procedures; or
 - C. Opposing any unlawful act or practice, provided that:
 - i. The individual or other person (including a DHS employee) has a good faith belief that the act or practice being opposed is unlawful; and
 - ii. The manner of such opposition is reasonable and does not involve a use or disclosure of an individual's protected information in violation of DHS policy.
 - D. Reporting a privacy incident in accordance with **DHS Policy DHS-090-005**.

3. Disclosures by whistleblowers

- a. A DHS employee or business associate may disclose an individual's protected client information if all three of the following circumstances are present before making a disclosure in the particular situation:
 - A. The DHS employee or business associate believes, in good faith, that DHS has engaged in conduct that is unlawful or that otherwise violates professional standards or DHS policy, or that the care, services, or conditions provided by DHS could endanger DHS staff, persons in DHS care, or the public; and
 - B. The disclosure is to:
 - i. An oversight agency or public authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of DHS;
 - ii. An appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or of misconduct by DHS; or
 - iii. An attorney retained by or on behalf of the DHS employee or business associate for the purpose of determining the legal options of the DHS employee or business associate with regard to this DHS policy and the disclosure is authorized

to be made under ORS 659A.200 to 659A.224 and not prohibited by ORS 659A.206(4) .

4. Disclosures by workforce crime victims or witnesses

- a. DHS workforce may disclose information about an individual to a law enforcement official if the staff is either the victim of a criminal act or a witness of criminal conduct on the premises of a DHS work place. DHS staff may disclose the facts and circumstances of the alleged crime, including such information the staff believes in good faith constitutes evidence of criminal conduct that occurred.
- b. In reporting criminal conduct, Department staff should refrain from identifying an alleged perpetrator as a client of the Department or from disclosing health or other information about the alleged perpetrator that is not directly pertinent to the actions of the alleged criminal conduct.

References

- 45 CFR 164.530
- [Privacy/Security Glossary of Common Terms](#)

Policy(ies) that apply:

[DHS-090-005](#) Privacy and Information Security Incident Response

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