

Policy Title:	Administrative, Technical, and Physical Safeguards				
Policy Number:	DHS-100-005	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 establish criteria for safeguarding confidential information and to minimize the risk of unauthorized access, use or disclosure.

Policy

1. General

DHS must take reasonable steps to safeguard information from any intentional or unintentional use or disclosure that is in violation of the privacy policies. Information to be safeguarded may be any medium including paper, electronic, oral and visual representations of confidential information.

2. Safeguarding confidential information - DHS workplace practices

a. Paper

- A. Each DHS workplace will store files and documents in locked rooms or storage systems.
- B. In workplaces where lockable storage is not available, DHS staff must take reasonable efforts to ensure the safeguarding of confidential information.
- C. Each DHS workplace will ensure that files and documents awaiting disposal or destruction in desk-site containers, storage rooms, or centralized waste/shred bins, are appropriately labeled, are disposed of on a regular basis, and that all reasonable measures are taken to minimize access.
- D. Each DHS workplace will ensure that shredding of files and documents is performed on a timely basis, consistent with record retention requirements.

b. Mail

- A. Each DHS workplace will ensure that mail is prepared accurately for delivery.
- B. Outgoing mail must include a complete sending address, including first and last name of recipient, agency name, and complete street and city address. If printed labels are not used, write or print legibly.

The outgoing mail must also include a complete return address (first and last name of sender, agency, complete street and city address).

c. Oral

- A. DHS staff must take reasonable steps to protect the privacy of all verbal exchanges or discussions of confidential information, regardless of where the discussion occurs.
- B. Each DHS workplace shall make enclosed offices and/or interview rooms available for the verbal exchange of confidential information.

Exception: In work environments structured with few offices or closed rooms, such as in the Oregon State Hospital, State Operated Group Homes or open office environments, uses or disclosures that are incidental to an otherwise permitted use or disclosure could occur. Such incidental uses or disclosures are not considered a violation provided that DHS has met the reasonable safeguards and minimum necessary requirements.

- C. Each DHS workplace must foster employee awareness of the potential for inadvertent verbal disclosure of confidential information.

d. Visual

- A. DHS staff must ensure that observable confidential information is adequately shielded from unauthorized disclosure on computer screens and paper documents.
 - i. Computer screens: Each DHS workplace must make every effort to ensure that confidential information on computer screens is not visible to unauthorized persons.
 - ii. Paper documents: DHS staff must be aware of the risks regarding how paper documents are used and handled, and must take all necessary precautions to safeguard confidential information.

e. Computer/electronic

- A. DHS staff who are assigned to use computers or electronic devices such as Blackberries are responsible for maintaining the security of passwords or other access methods.

3. Safeguarding confidential information – off-site DHS work practices

- a. All the safeguard requirements for the work place apply equally to any use of confidential information away from or off-site from the DHS work place. Files and records should be securely transported.
- b. Computer/electronic
 - A. DHS staff authorized to use laptop computers off-site are responsible for assuring the security, as well as minimized risk of loss, of the device and its contents.
 - B. DHS staff working on non-work shared computers should observe security protocols to prevent unauthorized users from accessing confidential information. Shared use of computers with family members or others who are not part of the DHS work force creates a risk of inadvertent disclosure of confidential information.
 - C. DHS staff are responsible for securing digital camera images. Digital cameras can store confidential information that can be accessed by anyone who has the camera.
- c. Telephone
 - A. DHS staff should ensure care when using telephones outside of the work space. Cell phones, Blackberry or other telephones require care to protect confidential information.
 - B. DHS staff should avoid using identifiable information about DHS clients unless staff have taken reasonable efforts to assure the privacy of the call.
- d. Safeguarding confidential information - DHS administrative safeguards
 - A. Implementation of role-based access and the Minimum Necessary Policy (**DHS-100-004**) will promote administrative safeguards.
 - i. Role Based Access Control (RBAC) is a form of security allowing access to data based on job function in accordance with DHS security procedures. Employees will be assigned to RBAC groups that will give members access only to the minimum necessary information to fulfill their job functions.
 - B. Conducting internal reviews periodically will permit DHS to evaluate the effectiveness of safeguards.
 - i. DHS managers and supervisors will conduct periodic reviews, under the direction of the DHS Information Security Office, in order to evaluate and improve the effectiveness of their current safeguards.

- C. Compliance with department-wide security policies will enhance administrative safeguards.
- D. Compliance with department-wide privacy policies and program-specific confidentiality and privacy requirements will enhance administrative safeguards.
- E. Training and periodic reminders to DHS staff about security and privacy are provided in an effort to enhance administrative safeguards.
- F. The established process for responding to security and privacy breaches and investigating causes of breaches permits DHS to continually respond to areas needing improvement and to improve its administrative safeguards, consistent with **Policy DHS-090-005**.

Procedures that apply

- None

References

- [Privacy/Security Glossary of Terms](#)

Policy(ies) that apply:

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

[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:

- 02/23/2005 - Administrative correction: Removed reference and link to "AS-100-005-01, Completing the DHS Safeguards Assessment Tool Procedure" as it has been obsoleted.
- 12/14/2004 - Administrative correction: Removed reference to the "Safeguards Guidance for DHS Managers" document that is no longer used.
- 03/31/2003 - Initial Release