Operational Policy

Policy Title:	**Administrative, Technical, and Physical Safeguards**		
Policy Number:	OHA-100-009		
Original Date:	7/22/2014	**Last Update:**	10/03/2016
Approved:	Mark Fairbanks, OHA CFO		

Purpose

This policy is one of a series that outlines Oregon Health Authority (OHA) guidelines and expectations for the necessary collection, use, and disclosure of protected information about individuals in order to provide services and benefits while maintaining reasonable safeguards to protect the privacy of their information.

Description

This policy describes the responsibility of OHA staff to maintain the privacy of an individual's protected information during day-to-day workplace practices, including awareness of information that may be disclosed in documents and conversations; ensuring the security of workplace surroundings; and ensuring the protection of information taken out of the work site.

Applicability

This policy applies to all OHA staff including employees, volunteers, interns and agency contractors.

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. OHA takes reasonable steps to safeguard information from any use or disclosure in violation of federal and state statute and rule and OHA privacy policies, regardless of how the information is conveyed: in hard copy, electronically or verbally.
2. OHA staff shall ensure that protected information is adequately shielded from unauthorized disclosure by:
    a. Being aware of information content and physical surroundings.
    b. Taking steps to follow OHA safeguards.
3. When information is created or maintained in hard copy, staff at each OHA work-site shall take all reasonable measures to minimize the possibility of unauthorized access.
    a. Hard copies of documents shall be stored in locked rooms or storage systems.

b. When information is in use, OHA staff shall make reasonable efforts to ensure protected information is not accessible to unauthorized users.
c. Centralized storage bins for protected materials shall be appropriately labeled and locked and materials disposed of on a regular basis.
d. Protected documents awaiting disposal or destruction in desk-site containers, or storage rooms shall be placed in locked centralized bins at the end of each day.
e. Shredding of stored files and documents shall be performed on a regular basis consistent with agency and program requirements.

4. OHA staff shall take reasonable steps to protect the privacy of all verbal exchanges of protected information, regardless of where the discussion occurs.
    a. Each OHA work-site shall make enclosed offices, interview rooms or meeting rooms available for the verbal exchange of protected information.
    b. Each OHA work-site shall foster workforce awareness of the potential for inadvertent verbal disclosure of protected information.
5. At work-sites structured with few offices or closed rooms, such as the Oregon State Hospital, state operated group homes or open office environments, verbal uses or disclosures that are incidental to an otherwise permitted use or disclosure are not considered a violation provided OHA has met the reasonable safeguards and minimum necessary requirements.
6. OHA staff shall lock electronic devices, including computers, cell phones and other personal or portable electronic devices if the devices are not in the area of the employee's immediate control.
7. OHA staff shall maintain the security of passwords or other access methods for electronic devices, including but not limited to computers, cell phones and other personal or portable electronic devices.
8. OHA staff shall comply with National Institute of Standards and Technology (NIST) Special Publications (SP) 800-111 and 800-88 for security of information.
9. OHA shall destroy PHI in a manner to render it unusable, unreadable, or indecipherable to unauthorized individuals in accordance with applicable retention policies.
10. OHA staff shall ensure that mail is prepared accurately for delivery.
    a. Outgoing mail shall have a complete mailing address that includes the first and last name of the recipient, agency name (if applicable), and the complete street and city address.
    b. Outgoing mail shall include a complete return address that includes the first and last name of the sender, the name of the agency, and the complete street and city address.
    c. If printed labels are not used, staff shall write or print legibly.
11. OHA staff shall ensure that email is prepared accurately for delivery.
    a. The intended recipient's email address shall be correctly entered.
    b. The subject line of an email should be general: it may provide insight into the subject matter but shall not include any personally identifying information, including an individual's name, birth date or OHP number.
    c. Any email containing protected information, including protected health information, shall be sent in a secured email.
    d. OHA staff requesting protected information be sent to them in an email shall send a secure email to the individual so the individual's information can be returned securely.
    e. To send a secured email, enter #secure# followed by a space and the subject of the email, in the subject line.
12. When using protected information away from the OHA work-site, OHA staff shall comply with all work-site security requirements.
13. OHA staff shall securely transport files and documents in accordance with the statewide Department of Administrative Services policy on Transporting Information Assets, agency policies and applicable program requirements.
    a. OHA staff who remove agency resources from the worksite, including protected or identifiable information, hard copy files, agency laptops, cell phones and other portable

electronic devices, shall assure the security of the resource and take steps to minimize risk of loss.
    i. OHA staff shall make every effort not to leave agency resources in a vehicle.
    ii. If no other option is available, agency resources left in a vehicle shall not be visible to a casual observer.
b. OHA staff authorized to remove protected or identifiable information in hard copy from the worksite shall maintain physical custody and control of the documents or secure the documents in a locked environment.
c. OHA employees using portable digital media or storage devices shall maintain physical custody and control or secure the device in a locked environment.
d. OHA shall encrypt all agency laptops and portable digital media or storage devices removed from OHA worksites.
e. OHA staff using non-agency computers shall observe appropriate security protocols to prevent unauthorized users from accessing protected information.

14. Verbal exchanges of protected information outside the work-site shall occur only when members of the workforce have taken appropriate steps to secure the privacy of the exchange.
15. OHA staff shall not post or share protected or personally identifying information about individuals on social media sites.
16. OHA uses role based access control (RBAC) and the minimum necessary standard to safeguard the privacy of protected information.
    a. RBAC is an administrative procedure that provides access to data based on job function in accordance with OHA security procedures.
    b. OHA assigns employees to RBAC groups that permit access to the minimum necessary information to fulfill their job functions.
17. OHA managers and supervisors shall conduct periodic internal reviews to evaluate and improve administrative safeguards, including ensuring that employees are assigned to the correct RBAC.
18. The Information Security and Privacy Office provides periodic training and reminders to OHA staff about security and privacy issues. Assistance or consultation are available upon request.
19. All staff shall take OHA privacy and security training on an annual basis.
20. OHA maintains an established process for responding to security and privacy breaches and determining the cause of breaches.
21. If OHA policy conflicts with federal or state statute or rule that statute or rule supersedes unless the OHA policy provides more protection.

References

DAS Transporting Information Assets 107-011-140
National Institute of Standards and Technology (NIST) Special Publication 800-111
NIST Special Publication 800-88
OHA Social Media Expectations and Responsibilities
OHA 100-014 Report and Response to Privacy and Security Incidents
Privacy/Security Glossary of Common Terms

Contacts

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

Policy History
Version 1 Established 7/22/2014
Reviewed 10/03/2016

To request this policy in another format or language, contact the Publications and Design Section at 503-378-3486, 711 for TTY, or email dhs-oha.publicationrequest@state.or.us

Keywords
Individual privacy, Protecting privacy, Authorization, Access, Privacy, Security, RBAC