CHAPTER 407
DEPARTMENT OF HUMAN SERVICES,
ADMINISTRATIVE SERVICES DIVISION AND DIRECTOR'S OFFICE

DIVISION 14
PRIVACY AND CONFIDENTIALITY

Access Control

407-014-0300
Scope

These rules (OAR 407-014-0300 through 407-014-0320) apply to an entity or individual seeking or receiving access to Department information assets or network and information systems for the purpose of carrying out a business transaction between the Department and the user.

(1) These rules are intended to complement, and not supersede, access control or security requirements in the Department's Electronic Data Transmission rules, OAR 407-120-0100 to 407-120-0200, and whichever rule is more specific shall control.

(2) The confidentiality of specific information and the conditions for use and disclosure of specific information are governed by other laws and rules, including but not limited to the Department's rules for the privacy of protected information, OAR 410-014-0000 to 410-014-0070.

Stat. Auth.: ORS 409.050
Stats. Implemented: ORS 182.122

407-014-0305
Definitions

For purpose of these rules, the following terms have definitions set forth below. All other terms not defined in this section shall have the meaning used in the Health Insurance Portability and Accountability Act (HIPAA) security rules found at 45 CFR § 164.304:

(1) "Access" means the ability or the means necessary to read, communicate, or otherwise use any Department information asset.

(2) "Access Control Process" means Department forms and processes used to authorize a user, identify their job assignment, and determine the required access.

(3) "Client Records" means any client, applicant, or participant information regardless of the media or source, provided by the Department to the user, or exchanged between the Department and the user.

(4) “Department” means the Department of Human Services.

(5) “Incident” means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of any network and information system or Department information asset including, but not limited to unauthorized disclosure of information; failure to protect user’s identification (ID) provided by the Department; or, theft of computer equipment that uses or stores any Department information asset.

(6) “Information Asset” means any information, also known as data, provided through the Department, regardless of the source or media, which requires measures for security and privacy of the information.

(7) “Network and Information System” means the State of Oregon’s computer infrastructure, which provides personal communications, client records, regional, wide area and local area networks, and the internetworking of various types of networks on behalf of the Department.

(8) “User” means any individual or entity authorized by the Department to access a network and information system or information asset.

Stat. Auth.: ORS 409.050
Stats. Implemented: ORS 182.122

407-014-0310
Information Access

The user shall utilize the Department access control process for all requested and approved access. The Department shall notify the user of each approval or denial. When approved, the Department shall provide the user with a unique login identifier to access the network and information system or information asset.

Stat. Auth.: ORS 409.050
Stats. Implemented: ORS182.122

407-014-0315
Security Information Assets

(1) No user shall access an information asset for any purpose other than that specifically authorized by the Department access control process.

(2) Except as specified or approved by the Department, no user shall alter, delete, or destroy any information asset.

(3) The user shall prohibit unauthorized access by their staff, contractors, agents, or others to the network and information systems, or Department information assets, and shall

implement safeguards to prevent unauthorized access in accordance with section (4) of this rule.

(4) The user shall develop a security risk management plan. The user shall ensure that the plan includes, at a minimum, the following:

(a) Administrative, technical and physical safeguards commonly found in the International Standards Organization 27002:2005 security standard or National Institute of Standards and Technology (NIST) 800 Series;

(b) Standards established in accordance with HIPAA Security Rules, 45 CFR Parts 160 and 164, applicable to a user regarding the security and privacy of a client record, any information asset, or network and information system;

(c) The user's privacy and security policies;

(d) Controls and safeguards that address the security of equipment and storage of any information asset accessed to prevent inadvertent destruction, disclosure, or loss;

(e) Controls and safeguards that ensure the security of an information asset, regardless of the media, as identified below:

(A) The user keeps Department-assigned access control requirements such as identification of authorized users and access control information (passwords and personal identification numbers (PIN's), in a secure location until access is terminated;

(B) Upon request of the Department, the user makes available all information about the user's use or application of the access controlled network and information system or information asset; and

(c) The user ensures the proper handling, storage, and disposal of any information asset obtained or reproduced, and, when the authorized use of that information ends, is consistent with any applicable record retention requirements.

(f) Existing security plans developed to address other regulatory requirements, such as Sarbanes-Oxley Act of 2002 (PL 107-204), Title V of Gramm Leach Bliley Act of 1999, will be deemed acceptable as long as they address the above requirements.

(5) The Department may request additional information related to user's security measures.

(6) The user must immediately notify the Department when access is no longer required, and immediately cease access to or use of all information assets or network and information systems.

Stat. Auth.: ORS 409.050
Stats. Implemented: ORS 182.122

407-014-0320
User Responsibility

The user shall not make any root level changes to any Department or State of Oregon network and information system. The Department recognizes that some application users have root level access to certain functions to allow the user to diagnose problems (such as startup or shutdown operations, disk layouts, user additions, deletions or modifications, or other operation) that require root privileges. This access does not give the user the right to make any changes normally restricted to root without explicit written permission from the Department.

(1) Use and disclosure of any Department information asset is strictly limited to the minimum information necessary to perform the requested and authorized service.

(2) The user shall have established privacy and security measures that meet or exceed the standards set forth in the Department privacy and information security policies, available from the Department, regarding user's disclosure of an information asset.

(3) The user shall comply with all security and privacy federal and state laws, rules, and regulations applicable to the access granted.

(4) The user shall make the security risk plan available to the Department for review upon request.

(5) The user shall report to the Department all privacy or security incidents by the user that compromise, damage, or cause a loss of protection to the Department information assets or the network and information systems. The incident report shall be made no later than five business days from the date on which the user becomes aware of such incident. The user shall provide the Department a written report to include the results of the incident assessment findings and resolution strategies.

(6) Wrongful use of a network and information system, or wrongful use or disclosure of a Department information asset by the user may cause the immediate suspension or revocation of any access granted, at the sole discretion of the Department without advance notice.

(7) The user shall comply with the Department's request for corrective action concerning a privacy or security incident and with laws requiring mitigation of harm caused by the unauthorized use or disclosure of confidential information, if any.

Stat. Auth.: ORS 409.050
Stats. Implemented: ORS182.122