DHS Oregon Department of Human Services **Vocational Rehabilitation**	**Information Memorandum Transmittal**

Authorization: Dan Haun **Number: VR-IM-15-6**

Policy/Program Development Interim **Issue date: July 9, 2015**

Topic: Confidential or private participant information disclosure

Subject: Verify identity of Oregon Vocational Rehabilitation participant prior to disclosing protected information

Applies to (*check all that apply*):

☒	**Vocational Rehabilitation - All Staff**
☐	Vocational Rehabilitation – Executive Team
☐	Vocational Rehabilitation – Administration
☐	Vocational Rehabilitation – Branch Managers
☒	Other (please specify) Contractors with Vocational Rehabilitation
☐	Other (please specify)

Reason for Transmittal:

A recent breach of protected information occurred in a Vocational Rehabilitation office. Vocational Rehabilitation staff involved in the breach did not report the incident to the Department of Human Services, Information Security & Privacy Office (ISPO) as required.

ISPO reports a recent increase in mishandled documents generally. "The risk for mishandling documents rises when workloads increase as a result of increased demand for services and increased work pace to respond to the demand. A lack of attention to detail when mailing, copying, producing documents, and hand delivering documents to clients or trainees also can result in errors." See: https://inside.dhsoha.state.or.us/asd/info-security/165-iso-alerts/3990-appropriate-handling-of-documents.html

This transmittal's purpose is to assure staff knows how to protect participant information as it arrives in the office, and, is later shared with the participant. Additionally staff will recognize a breach of security and report these incidents to ISPO.

Message:

Verify Identity of Participant Prior to Disclosure of Protected Information Two Times

First, confirm that the information sent is for the appropriate person. Upon receiving medical records and other personal health information with a vocational rehabilitation participant, Vocational Rehabilitation staff shall, to the best of his/her ability:

- Confirm that the protected information sent by the health provider matches with the name and other identifying information (full name and birth date or address) available on that individual **soon after it arrives in the office.**
- **If the wrong file was sent to you, return it and inform the organization to file a report** with the Information Security & Privacy Office. Provide contact information, if needed. ISPO documents these incidents.

Second, Vocational Rehabilitation staff confirms the information is for the participant served. When the counselor meets with the participant to share the protected information the counselor shall:

- **Before disclosing** the information to the participant, verify the information is for this individual. At a minimum, check that the individual's complete name and birth date or address match that of the protected information file.

If you are uncertain about the match between the protected information and the program participant at any point, please stop and confer with the branch manager.

- **If you disclose medical records and other personal health information inappropriately**, stop the process. Alert your supervisor immediately. If the incident involves your supervisor, you may report the incident

directly to the Information Security & Privacy Office. Gather as much detail about the incident as possible: date, time, location, type of information, contact information, etc.

How to File an Incident Report

Should a breach or disclosure of protected information occur at any point in service delivery, complete the Department of Human Services form **MSC 3001** (02/13 or a more recent version of this form) the DHS/OHA Privacy/Security Incident Report.

When providing a description of the incident always include information about the timeline, the specific information disclosed and to whom it was disclosed.

If you have questions about completing the form or discussing the situation, contact:

- The Program Technician for your office or branch,
- The Dispute Resolution Coordinator, or,
- The Policy Analyst.

For more information how to report a privacy or security incident, see: https://inside.dhsoha.state.or.us/asd/info-security/privacy.html

Information on this website follows this memo.

You may also contact the Information Security & Privacy Office (ISPO) via phone, email, fax, or in-person. They want to help you understand and follow the numerous requirements for protecting privacy and security of all Vocational Rehabilitation information. Additionally, the ISPO staff gathers and manages privacy and security incidents.

Information Security & Privacy Office (ISPO) Service Desk:

Privacy program phone: 503-945-5780

Fax 503-947-5396

Email dhs.privacyhelp@state.or.us

Information Security and Privacy Office intranet for employee:
http://inside.dhsoha.state.or.us/asd/info-security.html

Information and Security Privacy Office internet for partners:
http://www.oregon.gov/OHA/admin/infosec/index.shtml

Email dhs.privacyhelp@state.or.us

Background

The Privacy of Individually Identifiable Health Information (*45 CFR Parts 160 and 164)*

The federal regulations governing privacy of health information was effective April 14, 2001. This is the "Privacy Rule." Although Vocational Rehabilitation is not a health care provider, these guidelines in the Privacy Rule provide clear expectations for dealing with personal, protected health information.

Website for this information:
http://aspe.hhs.gov/admnsimp/final/pvcguide1.htm

Information from the above website provides these questions and answers.

Q: What does this regulation do?

A: The Privacy Rule became effective on April 14, 2001, requiring most health plans and health care providers covered by the new rule to comply with the new requirements by April 2003.

- The Privacy Rule for the first time creates national standards to protect individuals' medical records and other personal health information.
- It gives patients more control over their health information.
- It sets boundaries on the use and release of health records.
- It establishes appropriate safeguards that health care providers and others must achieve to protect the privacy of health information.
- It holds violators accountable, with civil and criminal penalties that can be imposed if they violate patients' privacy rights.
- And it strikes a balance when public responsibility requires disclosure of some forms of data - for example, to protect public health.

For patients - it means being able to make informed choices when seeking care and reimbursement for care based on how personal health information may be used.

- It enables patients to find out how their information may be used and what disclosures of their information have been made.
- It generally limits release of information to the minimum reasonably needed for the purpose of the disclosure.
- It gives patients the right to examine and obtain a copy of their own health records and request corrections.

Q: Why is this regulation needed?

A: In enacting the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Congress mandated the establishment of standards for the privacy of individually identifiable health information.

Before HIPAA was in place, our country has relied on a patchwork of federal and state laws to protect personal information that moved across hospitals, doctors' offices, insurers or third party payers, and state lines. Personal health information was distributed - without either notice or consent - for reasons that had nothing to do with a patient's medical treatment or health care reimbursement. Patient information held by a health plan may be passed on to a lender who may then deny the patient's application for a home mortgage or a credit card - or to an employer who may use it in personnel decisions. The Privacy Rule establishes a federal floor of safeguards to protect the confidentiality of medical information. State laws which provide stronger privacy protections will continue to apply over and above the new federal privacy standards.

Health care providers and service agency staff have a strong tradition of safeguarding private health information. The old system of paper records in locked filing cabinets is not enough. With information broadly held and transmitted electronically, the rule provides clear standards for all parties regarding protection of personal health information.

If you have any questions about this information, contact:

Contact(s):	Robin Brandt		
Phone:	503-945-5857	**Fax:**	503-947-5010
Email:	robin.l.brandt@state.or.us		

See: https://inside.dhsoha.state.or.us/asd/info-security/privacy.html

Privacy

Reporting a privacy or security incident

Please report all privacy and information security incidents to the ISPO.

Step 1 - Alert your supervisor to the problem immediately. If the incident involves your supervisor, you may report the incident directly to the Information Security & Privacy Office (see Step 3).

Note: If the incident involves the theft or loss of a DHS/OHA computer, laptop, or mobile device you must also:

- Report loss to the OIS Service Desk: (503) 945-5623. They are responsible for deactivating the device.
- If it involves theft, also notify your local law enforcement agency.

Step 2 - Gather as much detail about the incident as possible: date, time, location, type of information, contact information, etc. Download the Privacy Incident Report form DHS-3001 to assist in gathering the needed information. Completing the form is optional.

Step 3 - Report the incident to the DHS Information Security & Privacy Office (ISPO) via phone, email, fax, or in-person.

Phone 503-945-5780
Fax 503-947-5396
Email dhs.privacyhelp@state.or.us.

Incident Examples

An incident is a threat or event that compromises, damages, or causes a loss of confidentiality, integrity, or availability of DHS information or systems.

- **Privacy incidents**: Accidental or unauthorized acquisition, use, or disclosure of confidential or protected health information or personally identifiable information.
- **Security incidents**: The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information technology system.

Reportable examples

Description	Report to	Phone
Confidential information is accidentally or intentionally disclosed	ISO Privacy Program	503-945-5780
Unauthorized reproduction of confidential information	ISO Privacy Program	503-945-5780
Stolen or lost confidential client or employee information	ISO Privacy Program	503-945-5780
Lost or stolen equipment containing confidential information	ISO Security Program --and-- OIS Service Desk	503-945-6812 503-945-5623
Lost or stolen computer equipment or BlackBerry **not** containing confidential or protected information	ISO Privacy Program	503-945-5780
Sent confidential client information to a wrong provider, partner, or contractor outside of DHS	ISO Privacy Program	503-945-5780
Misdirected e-mail containing confidential client or staff information	ISO Privacy Program	503-945-5780
An unauthorized person asks for or is given access to DHS systems	ISO Privacy Program	503-945-5780
Employees sharing logins and/or passwords	ISO Privacy Program	503-945-5780
An employee asks for another	ISO Privacy Program	503-945-5780

employees password.		
Data is modified for unexplained reasons	ISO Privacy Program	503-945-5780
Data is defaced or destroyed without authorization, intentionally or accidentally	ISO Privacy Program	503-945-5780
Misuse or tampering with DHS equipment	ISO Security Program	503-945-6812
A workstation or notebook computer is found to have a virus	ISO Security Program --and-- OIS Service Desk	503-945-6812 503-945-5623
Found electronic equipment such as a camera or storage device (USB drive, CD/DVD, etc.) and the contents are unknown.	ISO Security Program	503-945-6812
Any violation of DHS privacy polices or information security policies.	ISO Privacy Program	503-945-5780

Last Updated (Wednesday, 25 March 2015 09:25)

ISPO

- ISPO Home
- **Privacy**
- Security
- Information Exchange
- Awareness & Education
  - Training
  - Tip Sheets
- How do I...?
  - Report an Incident
  - Mail processing and privacy
  - Password security
  - Phish sense
  - Send a secure email
  - Disposal of confidential information
- Tools and resources
- Communications
  - Email communication archive
  - ISO Newsletter archive
- Frequently Asked Questions
- Who is the ISPO?