

Oregon Department of Human Services Information Systems Training: Privacy and Security Guidelines

The following guidelines apply to all DHS training related to client or provider data or systems.

All DHS staff that provide training are responsible to:

- Review and deliver a copy of these guidelines at the beginning of every training session.
- Ensure that pre-printed training manuals and handouts contain fictitious or unidentifiable client and provider data only.
- When necessary to train using live client data, ensure participants are accessing with their appropriate security level, and are accessing only the “minimum necessary” information needed for the topic being trained to.
- Clearly advise participants when live client data is being used so that participants can apply the appropriate safeguards.
- Instruct participants to alert the trainer immediately should they identify a conflict of interest with the client identifiable information or data being displayed during the training. Consider using live data from a distant location, to reduce the likelihood a conflict of interest will arise. This may be more significant in rural or small communities.
- Whenever possible, utilize a training database containing fictitious data when training on entering sensitive and specially protected information (i.e. mental health, alcohol and drug, diagnosis, disability).
- Remind participants that the responsibility to protect the information rests with the participants, as well as the trainer.

All training participants are responsible to:

- Use their own RACF ID when using live production systems during a training session.
- Abide by all confidentiality rules and policies.
- Protect passwords.
- Lock assigned computers (ctrl/alt/delete, enter) when leaving the immediate area for any length of time.
- Promptly retrieve and secure any documents generated by a printer, fax, or copier during the training.
- Shut off assigned computers at the end of the day, unless instructed otherwise by a trainer who is taking responsibility to shut off computers.
- In accordance with DHS policy, protect or properly dispose of any paper documents containing real client or provider data that are generated during the training. To locate Information Privacy and Security policies visit [www.dhs.state.or.us/admin/info security](http://www.dhs.state.or.us/admin/info_security)

***All DHS staff are responsible to ensure the confidentiality
of client and provider information.***