



ESA Nondisclosure of Confidential Information Agreement – Non Employee

This form is for contractors and other non-DSHS employees.

Confidential Information

“Confidential Information” means information that is exempt from disclosure to the public or other unauthorized persons under Chapter 42.56 RCW or other federal or state laws. Confidential Information includes, but is not limited to, protected health information as defined by the federal rules adopted to implement the Health Insurance Portability and Accountability Act of 1996, 42 USC §1320d (HIPAA), and Personal Information.

“Personal Information” means information identifiable to any person, including, but not limited to, information that relates to a person’s name, health, finances, education, business, use or receipt of governmental services or other activities, addresses, telephone numbers, social security numbers, driver license numbers, other identifying numbers, and any financial identifiers.

Regulatory Requirements and Penalties

State laws (including RCW 74.04.060 and RCW 70.02.020) and federal regulations (including HIPAA Privacy and Security Rules; 42 CFR, Part 2; 42 CFR Part 431) prohibit unauthorized access, use, or disclosure of Confidential Information. Violation of these laws may result in criminal or civil penalties or fines. You may face civil penalties for violating HIPAA Privacy and Security Rules up to \$50,000 per violation and up to \$1,500,000 per calendar year as well as criminal penalties up to \$250,000 and ten years imprisonment.

Assurance of Confidentiality

In consideration for the Department of Social and Health Services (DSHS) granting me access to DSHS property, systems, and Confidential Information, I agree that I:

1. Will not use, publish, transfer, sell or otherwise disclose any Confidential Information gained by reason of this agreement for any purpose that is not directly connected with the performance of the contracted services except as allowed by law.
2. Will protect and maintain all Confidential Information gained by reason this agreement against unauthorized use, access, disclosure, modification or loss.
3. Will employ reasonable security measures, including restricting access to Confidential Information by physically securing any computers, documents, or other media containing Confidential Information.
4. Have an authorized business requirement to access and use DSHS systems or property, and view its data and Confidential Information if necessary.
5. Will access, use and/or disclose only the “minimum necessary” Confidential Information required to perform my assigned job duties.
6. Will not share DSHS system passwords with anyone or allow others to use the DSHS systems logged in as me.
7. Will not distribute, transfer, or otherwise share any DSHS software with anyone.
8. Understand the penalties and sanctions associated with unauthorized access or disclosure of Confidential Information.
9. Will forward all requests that I may receive to disclose Confidential Information to my supervisor for resolution.
10. Understand that my assurance of confidentiality and these requirements do not cease at the time I terminate my relationship with my employer or DSHS.

I further understand that I must protect Employment Security Department (ESD) information identified as private and confidential as required by RCW 50.13. If I fail to comply with the requirements listed below I may be subject to a \$5,000 civil penalty.

- a. Staff with access to ESD information may not make any unauthorized disclosure of private and confidential records or information about employers, clients/claimants, employees, or any other private or confidential records or information. Private and confidential ESD records and information includes, but is not limited to, names, social security numbers, employee wages or hours, unemployment insurance benefit records, Standard Industrial Classification (SIC) codes of individual employers, employer locations, and employer names.
- b. Staff with access to ESD information may not use private and confidential records or information for personal gain.
- c. Staff with access to ESD information shall refrain from the unauthorized access to, or disclosure of, data and information systems.

Frequency of Execution and Disposition Instructions

This form will be read and signed by each non-DSHS employee who has access to Confidential information, and updated at least annually. Provide the non-DSHS employee signor with a copy of this Agreement and retain the original of each signed form on file for a minimum of six years.

Signature

PRINT/TYPE NAME

NON-DSHS EMPLOYEE’S SIGNATURE

DATE