Washington State Department of Social & Health Services

Agreement on Nondisclosure of Confidential Information – 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 or as otherwise identified in RCW 42.56.230.

REGULATORY REQUIREMENTS AND PENALTIES

State laws (including RCW 74.04.060and 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.

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

Washington State Department of Social & Health Services
Transforming lives

Internet Access Request and Agreement

DSHS Administrative Policy 15.15, Use of Electronic Messaging Systems and the Internet, requires that this form be completed and signed by the requestor and his or her manager to obtain *and use* Internet Services provided by DSHS. **This form also addresses DSHS Administrative Policy 15.24 Social Media usage.** The requestor's unit will retain a copy of the completed form for three years past the employee's termination date.

PRINT REQUESTOR'S NAME	EMPLOYEE'S PERSONNEL ID NUMBER	PRINT SUPERVISOR'S NAME	PRINT ORGANIZATION

List of Prohibited Activities Relating to Internet Use

Internet access and services are provided for official DSHS business activities except occasional but limited use, as defined in Administrative Policy 15.15. Prohibited activities include, but are not limited to (ask your supervision/support person to explain any items you do not understand):

1. Accessing the Internet for personal business or personal interest use that includes, but is not limited to:
   - Ordering or selling items on the Internet, except as specifically approved by DSHS for business purposes;
   - Participating in any online contest, promotion, or sweepstakes;
   - Participating in non-business related chat groups, list servers (automatic distribution lists), or newsgroups;
   - Transmitting political material; and
   - Gambling, soliciting money for religious or political causes, or for non-DSHS events.
2. Creating, posting, transmitting, or voluntarily receiving;
   - Obscene or pornographic material (except for official DSHS investigative activities);
   - Offensive, libelous, threatening, or harassing material; and
   - Degrading statements based on race, national origin, gender, sexual orientation, age, disability, religious, or political beliefs.
3. Linking DSHS web sites to other Internet sites whose content may be in violation of the mission or policies of DSHS.
4. Establishing a connection between a workstation connected to a DSHS network and an Internet service provider (ISP), such as Comcast, Quest, AOL, and MSNetwork, where the connection bypasses the WaTech firewall. This can occur when a modem and telephone line is used to establish the connection with the ISP.
5. Using e-mail products other than those provided and supported by the department. The prohibited products include third-party products on the Internet, e.g., Gmail, Hotmail, Juno, and AOL. Checking personal e-mail using department networks and communication lines is also prohibited because of the risk of computer viruses.
6. Storing department data on disk storage devices operated by vendors over the Internet unless in accordance with DSHS Information Security Policy Manual, Section 5.1.
7. Using state provided equipment or Internet connectivity to perform any illegal activities, e.g., deliberately spreading viruses, gaining unauthorized access to another computer, or making another network unusable by launching a denial of service attack.
8. Transmitting unencrypted sensitive or confidential department information over the Internet.

DSHS employees and other workers must adhere to Administrative Policy 15.24 Social Media Policy as it prohibits non-business personal use of social media during business hours or using department resources (time and equipment).

Statement of Agreement

I have read, understand and will comply with DSHS Administrative Policies 15.15, Use of Electronic Messaging Systems and the Internet, and 15.24 Social Media Policy and the list of prohibited activities above. I also understand that failure to comply with the established policies can result in disciplinary action, up to and including dismissal from employment or more serious consequences (e.g., criminal charges).

REQUESTOR'S SIGNATURE	DATE
SUPERVISOR'S SIGNATURE	DATE
APPROVED BY (ADDITIONAL SIGNATURE, IF REQUIRED)	DATE

Copy To: Individual's personnel file

FOR IMAGING ONLY	PERSONNEL ID	DOC DATE	SECTION	DOC TYPE	SUB DOC TYPE	HR REP
			Training	Form	Internet Request	

Washington State Department of Social & Health Services
Transforming lives

DSHS Nondisclosure of Confidential Information

Confidential Information

Department of Social and Health Services (Department) employees may need access to or come into contact with confidential information from different DSHS programs, from business partners, and from the Health Care Authority (HCA), the Department of Children, Youth, and Families (DCYF), and from other state and Federal agencies. Confidential information includes, but is not limited to, personal information about individual clients and employees, such as names, social security numbers, protected health information (PHI), services or benefits received and other information identifying individual clients that is protected by law and not available to the general public.

As a Department employee, I have reviewed and understand:

1. The Department's requirements for protecting confidential information, explained in Administrative Policy 5.01;
2. The penalties and sanctions associated with unauthorized access, use, or disclosure of confidential information; and
3. My responsibility to keep confidential information and computer systems secure, as explained in the department's required Information Technology Security Awareness Course (available on-line in the DSHS Learning Center).

Requirements and Penalties

State laws applicable to Department programs (including RCW 74.04.060, Chapter 13.50 RCW; and Chapter 70.02 RCW) and federal regulations (including Federal Tax laws - 26 USC ss.7213, 7213A, 7431; Federal laws for protection of National Directory of New Hires (NDNH) information received from the Office of Child Support Enforcement (OCSE) 42 USC § 653 (l); Administrative procedures for individual records- 5 USC § 552a (i); HIPAA Privacy and Security Rules, the Social Security Act, and chemical dependency rules at 42 CFR, Part 2) prohibit unauthorized access, use, or disclosure of confidential information. Civil penalties for violations of HIPAA Privacy and Security Rules may be imposed up to $50,000 per violation for a total of up to $1,500,000 for violations of each requirement during a calendar year. Criminal penalties may total up to $250,000 and ten years imprisonment.

Employee Assurance of Confidentiality

As a condition of my employment with the Department of Social and Health Services (DSHS), I commit and agree to be bound by the following:

1. I certify I will not access or use confidential information unless directly related to my assigned job duties and will not use confidential information for personal purposes or gain.
2. I agree not to disclose confidential information to any unauthorized person or entity, either orally, in writing, or by electronic means and agree to protect information as required by agency privacy and security policies
3. I understand I am authorized to access, use and/or disclose only the "minimum necessary" confidential information required to perform my assigned job duties.
4. I understand that I am not allowed to store confidential information on personal devices or systems not provided and authorized by DSHS.
5. I understand that it is my responsibility to report any and all suspected or actual unauthorized access, loss, theft or disclosure of confidential information (breaches).
6. If I have questions or am uncertain about requests for confidential information I receive, I will forward them to my supervisor for resolution.
7. I understand these requirements and my assurance of confidentiality do not cease at the time my employment ends with DSHS.

Frequency of Execution and Disposition Instructions

This form will be executed by each employee and updated annually. Provide the employee with a copy of this form and retain the original of each signed form in the employee's personnel file for a minimum of six years.

Holders of Employment Security Department (ESD) Information

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.

1. 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.
2. Staff with access to ESD information may not use private and confidential records or information for personal gain.
3. Staff with access to ESD information shall refrain from the unauthorized access to, or disclosure of, data and information systems.

Signatures

EMPLOYEE'S SIGNATURE	DATE	PRINT NAME	PERSONNEL ID NUMBER
SUPERVISOR'S SIGNATURE	DATE	PRINT SUPERVISOR'S NAME	

FOR IMAGING ONLY	PERSONNEL ID	DOC DATE	SECTION	DOC TYPE	SUB DOC TYPE	HR REP
			Training	**Form**	**Non-Disclose Confidential**	

Washington State Department of Social & Health Services
Transforming lives
Behavioral Health Administration
WESTERN STATE HOSPITAL

Acknowledgement of Healthcare Screening For Contractors

In consideration of being granted access ***to Eastern State Hospital (ESH)*** or its Patients, or to perform duties or services under a Contract with the Washington State Department of Social and Health Services, I acknowledge that I:

- Have had a TST (tuberculin skin test) or IGRA (Interferon Gamma Release Assay) within the past 12 months;

OR

- Have a current chest x-ray and documentation of a TB Symptom Assessment. If positive TST or IGRA and agree to have a TB Symptom Assessment documentation performed annually thereafter.

AND

- Have current immunizations or titers evidencing immunity, or a signed declination for vaccination against Hepatitis B, MMR and Varicella (chickenpox). Tdap (Tetanus with Whooping Cough) vaccination is highly recommended but not mandatory.

AND

- Am vaccinated against COVID-19 and agree to provde proof of COVID-19 vaccination with me when I attend initial NEO orientation at ESH for verification purposes. The Hospital is unable to offer accommodations to contractor personnel with COVID-19 vaccination exceptions who perform duties or services at ESH.

I further acknowledge that I shall provide proof of compliance with any of the above requirements upon request from ESH within 24 hours of such request.

I can be reached at _____ when documents are required.

I shall comply with all health screening requirements communicated to me by Eastern State Hospital prior to providing in-person or on-site duties or services at the Hospital; and shall provide upon request from ESH, at my expense, satisfactory evidence of required immunizations, titers, TB testing results, and declinations or exempt status.

Contractor Name:		
Contracted Staff Signature:	Printed Name:	Date:

For questions regarding this form, contact:
ESH Contract Management Dept. 509.565.4301, Dana.Martin@dshs.wa.gov

Eastern State Hospital Computer Network Access Request

Date of Request: _____

Name (Last) _____, (First) _____ (MI) ___

Any Nickname or ***Known As*** name info: _____

Position Title: _____

Department or Ward: _____

Work area phone number: _____

Assigned Shift: ☐ Day ☐ Eve ☐ Night

Supervisor Name: _____

State Employee ID #: | | | | | | | | |

---------- PLEASE DO NOT WRITE BELOW THIS LINE ----------

User Name: | | | | | | | |

AD Account created initial and date: _____

Temp password assigned: _____

Exchange Account created initial: _____

OWA set to disabled: _____

The following DSHS forms have been completed and scanned into personnel file:

☐ DSHS 03-344 Internet Access Request and Agreement

☐ DSHS 03-374 DSHS Nondisclosure of Confidential Information

Pyxis MEDSTATION®
Password Verification Statement

The first time you access a MEDSTATION® you will be required to enter a new, confidential password. It is your responsibility to keep your password secret. You will be accountable for all transactions performed using this User ID and password.

Please read the following statement and sign at the bottom to verify that you have read and understood the statement:

> I understand that my User ID, in combination with my confidential password, will be my electronic signature for all transactions in the Pyxis MEDSTATION® System. I understand that no retrievable record of my confidential password exists. All of my transactions on the MEDSTATION® will be permanently recorded with my User ID and a time-stamp and date. These records will be maintained and archived as per the policies of the hospital, and will be available for inspection by the Drug Enforcement Agency (DEA) and the State Board of Pharmacy, as is presently done with my handwritten signature for controlled substance records.

I understand that to maintain the integrity of my electronic signature, I must not give this password to any other individual.

_____ _____

Signature of Pyxis User Date

_____

Printed Name

_____ _____

Supervisor's Authorization Date