

PRISM Access Request

An Organization may request access to PRISM for its employees or employees of Subcontractors (**Users**) under its Data Share Agreement (DSA) with DSHS and HCA. The Organization **PRISM Lead** reviews and completes the "Requesting Organization" section. The PRISM Access Request form must be signed by the **PRISM Lead** authorizing the request, which attests to the **Users'** business need for electronic Protected Health Information, and in the case of a Subcontractor User, attests that the contract with the Subcontractor includes a HIPAA Business Associate Agreement and Medicare data share language, as appropriate. The **User** completes the "User Registration Information" section below and signs the "User Agreement and Non-Disclosure of Confidential Information" page. The **PRISM Lead** then forwards the request to: PRISM.Admin@dshs.wa.gov.

Upon review and acceptance, DSHS and HCA will grant the appropriate access permissions to the User and notify the **PRISM Lead**.

Changes to Access for Users

The **PRISM Lead** must notify the **PRISM Administrator** within five (5) business days whenever a **User** with access rights leaves employment or has a change of duties such that the User no longer requires access. If the removal of access is emergent, please include that information with the request.

Requesting Organization (to be completed by PRISM Lead)			
CONTRACTOR'S NAME		SUBCONTRACTOR'S NAME (IF APPLICABLE)	
CONTRACTOR'S STREET ADDRESS		CITY	STATE ZIP CODE
User Registration Information (to be completed by User)			
USER'S NAME (FIRST, MIDDLE, LAST)		USER'S JOB TITLE	
USER'S BUSINESS EMAIL ADDRESS		USER'S BUSINESS PHONE NUMBER (INCLUDE AREA CODE)	
Completion of HIPAA Training and IT Security Training in the past year:	DATE HIPAA TRAINING COMPLETED	DATE IT SECURITY TRAINING COMPLETED	
If user will be completing Health Action Plans (HAPs), enter the date HAP training was completed:	DATE HAP TRAINING COMPLETED		
PRISM USER'S SIGNATURE		DATE	PRISM USER'S PRINTED NAME
Authorizing Signature			
<p>Protected Data Access Authorization</p> <p>The HIPAA Security rule states that every employee that needs access to electronic Protected Health Information (ePHI) receives authorization from an appropriate authority and that the need for this access based on job function or responsibility is documented. I, the undersigned PRISM Lead, verify that the individual for whom this access is being requested (User or Subcontractor User) has a business need to access this data, has completed the required HIPAA Privacy training and the annual IT Security training and has signed the required <i>User Agreement and Non-Disclosure of Confidential Information</i> included with this Access Request. This User's access to this electronic Protected Health Information (ePHI) is appropriate under the HIPAA Information Access Management Standard and the Privacy Rule. In addition, if applicable, this employee has been instructed on 42 Code of Federal Regulations (CFR) Part 2 that governs the use of alcohol and drug use information and is aware that this type of data must be used only in accordance with these regulations. I have also ensured that the necessary steps have been taken to validate the User's identity before approving access to confidential and protected information. If a Subcontractor is indicated, I attest that the contract with the Subcontractor includes a HIPAA Business Associate Agreement, and where appropriate Medicare data share language.</p>			
PRISM LEAD SIGNATURE		DATE	PRISM LEAD NAME (PRINT)

User Agreement and Non-Disclosure of Confidential Information

Your Organization has entered into a Data Share Agreement (DSA) with the state of Washington Department of Social and Health Services (DSHS) and Health Care Authority (HCA) that will allow you to access data and records that are deemed Confidential Information as defined below. Prior to accessing this Confidential Information you must sign this **User Agreement and Non-Disclosure of Confidential Information** form.

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 and Personal Information.

“Protected Health Information” means information that relates to: the provision of health care to an individual; the past, present, or future physical or mental health or condition of an individual; or the past, present or future payment for provision of health care to an individual and includes demographic information that identifies the individual or can be used to identify the individual.

“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, credit card numbers, any other identifying numbers, and any financial identifiers.

Regulatory Requirements and Penalties

State laws (including, but not limited to, RCW 74.04.060, RCW 74.34.095, RCW 70.02.020 and RC2.70.02.230) and federal regulations (including, but not limited to, HIPAA Privacy and Security Rules, 45 CFR Part 160 and Part 164; Confidentiality of Alcohol and Drug Abuse Patient Records, 42 CFR, Part 2; and Safeguarding Information on Applicants and Beneficiaries, 42 CFR Part 431, Subpart F) prohibit unauthorized access, use, or disclosure of Confidential Information. Violation of these laws may result in criminal or civil penalties or fines.

User Agreement and Assurance of Confidentiality

In consideration for DSHS and HCA granting me access to PRISM or other systems and the Confidential Information in those systems, I agree that I:

- 1) Will access, use, and disclose Confidential Information only in accordance with the terms of this Agreement and consistent with applicable statutes, regulations, and policies.
- 2) Have an authorized business requirement to access and use DSHS or HCA systems and view DSHS or HCA Confidential Information.
- 3) Will not use or disclose any Confidential Information gained by reason of this Agreement for any commercial, personal, or research purpose, or any other purpose that is not directly connected with client care coordination and quality improvement.
- 4) Will not use my access to look up or view information about family members, friends, the relatives or friends of other employees, or any persons who are not directly related to my assigned job duties.
- 5) Will not discuss Confidential Information in public spaces in a manner in which unauthorized individuals could overhear and will not discuss Confidential Information with unauthorized individuals, including spouses, domestic partners, family members, or friends.
- 6) Will protect all Confidential Information against unauthorized use, access, disclosure, or loss by employing reasonable security measures, including physically securing any computers, documents, or other media containing Confidential Information and viewing Confidential Information only on secure workstations in non-public areas.
- 7) Will not make copies of Confidential Information, or print system screens unless necessary to perform my assigned job duties and will not transfer any Confidential Information to a portable electronic device or medium, or remove Confidential Information on a portable device or medium from facility premises, unless the information is encrypted and I have obtained prior permission from my supervisor.
- 8) Will access, use or disclose only the “minimum necessary” Confidential Information required to perform my assigned job duties.
- 9) Will protect my DSHS and HCA systems User ID and password and not share them with anyone or allow others to use any DSHS or HCA system logged in as me.
- 10) Will not distribute, transfer, or otherwise share any DSHS software with anyone.
- 11) Will forward any requests that I may receive to disclose Confidential Information to my supervisor for resolution and will immediately inform my supervisor of any actual or potential security breaches involving Confidential Information, or of any access to or use of Confidential Information by unauthorized users.
- 12) Understand at any time, DSHS or HCA may audit, investigate, monitor, access, and disclose information about my use of the systems and that my intentional or unintentional violation of the terms of this Agreement may result in revocation of privileges to access the systems, disciplinary actions against me, or possible civil or criminal penalties or fines.
- 13) Understand that my assurance of confidentiality and these requirements will continue and do not cease at the time I terminate my relationship with my employer.

User's Signature

PRISM USER'S SIGNATURE

DATE

PRISM USER'S PRINTED NAME