Washington State Department of Social & Health Services
Transforming lives

DSHS / HCA Systems Access Request

Washington State Health Care Authority

A DSHS HCS or DDA manager may request access to PRISM, ProviderOne and/or IPOne, for users, case managers, or contractors under the Data Share Agreements (DSA). This Access Request form must be signed by the employee's supervisor (Authorizer) and sent to their SSPS Coordinator after an EASE request has been submitted. Submit changes in employment status via EASE and using this form at least ten (10) business days prior to the change. ProviderOne and PPL access may take longer than ten days. If the removal of access is emergent, please include that information with the request.

☐ Check that an EASE Request has been submitted for the user.

REQUEST TYPE	USER'S ADMINISTRATION / DIVISION AND ADDRESS	STATE OFFICE DATE RECEIVED
☐ New user access ☐ Update user access ☐ Remove user access ☐ Change user name		REQUESTED USER ID

CHECK THE BOX FOR EACH SYSTEM ACCESS REQUESTED

☐ PRISM ☐ ProviderOne View Only

☐ IPOne – CM Role ☐ IPOne – HCRR Role ☐ IPOne – HQ Role ☐ IPOne – Other (specify role):

User Information

LAST NAME	FIRST NAME	MIDDLE INITIAL	DATE OF BIRTH	PHONE NUMBER (AREA CODE)

EMPLOYEE ID NUMBER	OFFICE	PRIOR NAME (IF CHANGE USER NAME REQUEST)

TITLE	INDIVIDUAL EMAIL ADDRESS (NO GENERIC EMAIL ADDRESSES)

ACCESS JUSTIFICATION

Protected Data Access Authorization

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 Authorizer, verify that the individual for whom this access is being requested has a business need to access this data, has completed the required HIPAA training and the annual IT Security training and has signed the required User Agreement on System Usage and Non- Disclosure of Confidential Information included with this Access Request. This user's access to this information is appropriate under the HIPAA Information Access Management standard. In addition, this employee has been instructed on 42 Code of Federal Regulations (CFR) Part 2 that governs the use of alcohol and drug abuse 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.

Authorizing Signature

SUPERVISOR'S (AUTHORIZER'S) SIGNATURE	DATE	PRINTED NAME	EMAIL ADDRESS

DSHS User Agreement on System Usage and Non-disclosure of Confidential Information

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

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, and RCW 70.02.020) 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 Assurance of Confidentiality

In consideration for DSHS and HCA granting me access to the PRISM, ProviderOne, 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 or personal purpose, research, 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.

Signature

USER'S SIGNATURE	DATE	USER'S PRINTED NAME