

## WITS Access Guidelines

Access to WITS is a privilege granted by the Division of Behavioral Health (DBH) and shall conform to the Division's EHR Information Management Policy (11-21). The following instructions provide direction on who may be granted access to WITS and the procedure for granting access.

The nature and extent of authorized access to WITS shall be determined by (a) legitimate need to fulfill job responsibilities; (b) local/state/federal/funding requirements; (c) confidentiality requirements; and (d) security requirements. Individuals with access to WITS are responsible for all actions and transactions occurring during their use of WITS.

Categories of individuals who may be granted access to the WITS Electronic Health Record (EHR) are:

- Staff of DBH who are performing a DBH function that requires information from the EHR to perform that job as approved by their supervisor. In these situations, access will be limited by job description or by specific activity to specific parts of the EHR
- Staff of agencies under contract with DBH who are performing a function for DBH that requires information/access to the EHR to perform that job, as approved by the DBH point-of-contact. In these situations, access may be limited by job description or to specific parts of the EHR.
- Student interns or volunteers who are performing a function for DBH that requires information/access to the EHR to perform certain duties, as approved by their DBH supervisor. In these situations, access will be issued by job description or to specific parts of the EHR
- Other Department of Health and Welfare staff may be granted access on an as needed basis

Categories of access to the EHR may include:

- Full access to health data, including clinical data, billing data, and medical data
- Limited access to a specific program or age group, specific time duration, specific client record, and/or other specific requests for information (e.g., by security access level)
- Functional limitation access such as view only, dictation access, or read-only Access

EHR access shall be terminated if an individual:

- is no longer a student, employee, or contractor affiliated with DBH
- no longer requires access for the performance of a job at DBH

EHR access may be terminated if an individual violates the EHR Information Management policy. The decision to terminate a user's access will be a joint decision between the Regional Hub Administrator and the Program Manager of Quality Assurance. Factors to consider regarding termination of access include but are not limited to:

- the individual's work responsibilities and need for access
- the severity of the policy violation
- other disciplinary sanctions that are imposed

DBH staff given access to the EHR shall follow the Administrative, Technical, and Physical safeguards outlined in the DHW Privacy and Confidentiality Manual. In addition, DBH will apply the following EHR security practices:

- *Individual authentication of users.* In order to establish individual accountability for actions on-line and to implement access controls based on individual needs, every individual shall have a unique identifier or log-on ID for use in logging into the EHR. All EHR users must protect their log-in or sign-in from unauthorized access. The user is prohibited from sharing individual security information with others and must report breaches of login or sign-in security immediately. Passwords/pins should include randomization of letters, numbers and other characters. It is recommended that names, words and common acronyms not be used as passwords/pins. Passwords/pins shall be changed according to the frequency identified by the EHR.
- *Access controls.* Users will only be given access to retrieve information for which they have a legitimate need to know. For example, users should only access client information needed to complete their job functions, even if they have access to other client information.
- *Physical security.* Users should (a) limit unauthorized physical access to computer systems, displays, networks and health-care records; (b) position monitors and keyboards so they are not easily seen by anyone other than the user; (c) where appropriate, program workstations to display passworded screen savers if left idle for a specified period of time.
- *Protection of external electronic communications.* In order to prevent interception by unauthorized individuals and protect client information the EHR shall only be accessed in secure/private areas. Do not access the EHR using an open public network (e.g. coffee shops).

DBH will apply the following organization practices:

- *Regional security.* Each Region will assign two Regional WITS Administrators (RWA) who have the responsibility to oversee the EHR system for the Regional Behavioral Health Center. The RWA will manage all DBH employees, volunteers, contractors, and external auditors who are given access to the EHR. The RWA will have the sole responsibility for granting and removing access privileges to/from users. For a complete list of RWA responsibilities please reference the Regional WITS Administrator Responsibilities checklist.
  - **Granting access:** Any individual (employee, student, volunteer, contract worker, or other non-employee) accessing the EHR must complete the WITS Security Request form and indicating that he or she will comply with privacy and confidentiality guidelines as outlined in HIPPA and CFR 42. This form should be signed *prior to* access being granted. The RWA shall ensure the signing of these agreements and keep the forms on file.
  - Employees engaged in any DBH activity who require access to the EHR shall complete and submit the following to the RWA: (a) WITS Security Request form; (b) Privacy and Confidentiality training certificate; (c) HIPPA training certificate; and (d) signed Privacy and Confidentiality Education & Compliance Agreement

- The RWA will review the request and compare requested access to the user's job responsibilities. The RWA shall note any access that could potentially create conflicts as defined by DBH business rules and follow up with the user's supervisor to request additional information. All requests for elevated privileges must be documented on the WITS Security Request form. The form should provide a business justification for the elevated privileges and be authorized by the appropriate supervisor.
- Once the RWA has approved the request, the RWA will set up the user account in WITS. Within five (5) business days of the creation of a WITS account, the RWA will create an *Account Administration* support ticket in WITS documenting the access and attach the WITS Security Request form. The Central Office WITS Administrator will review the form, verify the account settings and document it in the notes section of the support ticket. Modifications to an existing user access shall be documented using the same process as new user access.
- **Removing access:** Supervisors are responsible to notify the RWA of any termination of employment, internship, contract relationship, etc. so that timely termination of access to the EHR can be completed by the RWA. RWA's shall track and report termination of access to Central Office by creating a production support ticket indicating access has been terminated and the reason for the termination.
- *Education and training programs.* Each Region shall establish formal EHR training programs to ensure that all users of the information system understand how to use the system. Prior to being given EHR access, all DBH employees shall be trained on the EHR system and complete the following:
  - IDHW Privacy and Confidentiality Course located on the Knowledge and Learning Center (KLC). The employee must provide the certificate of completion to their immediate supervisor and the RWA.
  - Health Insurance Portability and Accountability Act (HIPAA) Course located on the KLC. The employee must provide the certificate of completion to their immediate supervisor and the RWA.
  - Review the IDHW Privacy and Confidentiality Manual and sign the Acknowledgment of Privacy/Confidentiality Education & Compliance Agreement. The employee must provide a signed copy of the agreement to their immediate supervisor and RWA.
  - Any specialized training to access certain areas of the EHR (e.g., CAFAS, GAIN-I, CA/LOCUS, etc.).
  - Contract users must provide written verification from their agency that they have been trained in confidentiality, privacy and HIPAA.

**Any and all questions regarding access to WITS shall be directed to the WITS Help Desk at 208 334-5673, Option 2 or [DBHWITSHD@dhw.idaho.gov](mailto:DBHWITSHD@dhw.idaho.gov).**