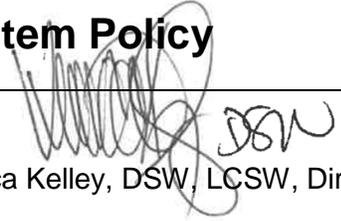




# Electronic Health Record (AVATAR) System Policy

**Effective Date** 06/14/2019  
**Approved Date** 06/14/2019

  
Veronica Kelley, DSW, LCSW, Director

**Policy** It is the policy of the Department of Behavioral Health (DBH) to maintain an electronic health record system (EHR) for the treatment of behavioral health system clients in a manner that ensures access, receipt and transmission of protected health information (PHI) is conducted securely with no access to unauthorized individuals. DBH Information Technology (IT) and Security Officer will ensure the ongoing implementation and maintenance of EHR features, updates, access controls and other required activities are in accordance with privacy and safeguard practices as specified in 45 CFR Section 164, subpart C, 45 CFR Section 164.316, and 42 CFR Part 2.13 and 2.16.

**Purpose** This policy outlines the required practices and oversight in accordance with relevant administrative, technical and physical safeguards mandated by state and federal privacy laws for mental health and substance use disorder electronic health records.

**Definition(s)** **Access Control:** The act of limiting a user’s access to certain data based on role, job function, and client population;

**Account Creation:** The process of creating an account on a computer system and granting the user/workforce member permission to access or use of a subset of files or data. EHR accounts are comprised of the following components:

**User ID:** A unique identifier assigned to a workforce member’s account. This typically contains the employee number.

**Password:** A secret unique combination of characters that is selected by the individual/workforce member based on password complexity requirements that grants access to the computer or network.

**Role:** A pre-defined set of rules that enables access to selective information in EHR’s database.

*Continued on next page*

## Electronic Health Record (AVATAR) System Policy, Continued

---

**Definition(s),**  
continued

**Confidential Data:** Includes, but is no limited to, PHI and is information that is sensitive, proprietary, or personal to which access must be restricted and whose unauthorized disclosure, theft or improper use could be harmful to a person, process, or the organization. Data or information that is regarded as sensitive must be disseminated only to an individual or organization authorized to access it;

**Disclosure:** The release, transfer, provision of access to, or dividing in any other manner of, PHI outside the covered entity holding the information;

**Protected Health Information (PHI):** Individually identifiable health information that is transmitted or maintained in any form or medium (electronic, paper, microfiche or verbal);

**Remote Access:** The ability to gain access to the DBH's network from outside the network's perimeter. Remote access to EHR is a privilege granted through the user provisioning process to workforce members as approved by DBH's management. Remote access granted to DBH workforce members will be restricted to the minimum necessary information required to carry out job responsibilities, terms of contracts, agreements, or as further defined by DBH management;

**Unauthorized Access:** in appropriate access, review or viewing of client medical information without direct need for medical diagnosis, treatment or other unlawful use not permitted by either CMIA, or by other Statutes or regulations governing the lawful access, use or disclosure of medical information;

**Use:** With respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within a covered entity that maintains such information;

**Workforce Member(s):** Employees, volunteers, trainees, students, and other persons whose conduct, in the performance of work for a covered entity, I s under the direct control of such entity, whether or not they are paid by the covered entity.

---

*Continued on next page*

## Electronic Health Record (AVATAR) System Policy, Continued

---

### Account Creation and Monitoring

The DBH EHR is a web-based application utilized during the delivery of direct services and/or other engagement with a behavioral health system of care client. The EHR consists of two separate portals for the engagement/treatment and record retention of Mental Health (MH) and Substance Use Disorder (SUD) clients. The two separate portals ensure access to each is appropriate for the individual user, and in accordance with SUD privacy law, 42 CFR Part 2.

User account profile types are created based on area assigned (MH or SUD), as well as the discipline and position type. Profile types will be approved by DBH Security Officer and Privacy Officer, as well as account profile creation requests that are not standard and are unique based on the specialty assignment (e.g., Community Crisis Response staff, clinicians assigned to both MH and SUD clients, etc.)

DBH user accounts are closely monitored and maintained to prevent unauthorized access of data by the Security Officer or designee.

Account creation shall be completed for authorized individuals' limiting access according to each individual's verified business need employing DBH access control standards. Regular monitoring of DBH users will be conducted by DBH Security Officer or designee to determine any unauthorized access, disclosure, and/or use of client PHI. All suspected or actual violations or access or disclosure will be reported immediately to the DBH Office of Compliance for appropriate investigation, remedial action and reporting as outlined in DBH Fraud, Waste and Abuse Policy (COM 0927).

Prospective users must complete the following prior to access being granted:

#### 1. Training:

Course
HIPPA Privacy and Training (Relias)
EHR Training Course (Workforce & Education Training)

---

*Continued on next page*

## Electronic Health Record (AVATAR) System Policy, Continued

---

**Account Creation and Monitoring,**  
continued

### 2. Acknowledgement and Completion of:

<b>Policies and Form</b>
Computer Network Appropriate Use Policy (IT 5004)
Remote Access Policy (IT 5006)
Confidentiality of Protected Health Information (PHI) (COM 0905)
Compliance Verification, Monitoring and Auditing Policy (COM 0917)
Oath of Confidentiality Form or
Oath of Confidentiality Form (for Contract Providers and Business Associates)

---

**Related Policy or Procedure**

- Confidentiality of Protected Health Information (PHI) (COM 0905)
  - Compliance Verification, Monitoring and Auditing Policy (COM 0917)
  - Computer and Network Appropriate Use Policy (IT 5004)
  - Remote Access Policy (IT 5006)
- 

**Reference(s)**

- 45 CFR 164.502(b) and 164.514(d) Minimum Necessary
  - Health Insurance Portability and Accountability Act of 1996 (HIPAA)
  - Health Information Technology for Economic and Clinical Health Act (HITECH)
  - 42 CFR Part 2 Final Rule
-