

## Data System Access Management

### ***Policy***

It is the policy of Central Florida Behavioral Health Network, Inc. (CFBHN) to maintain formal procedures that define the methods by which staff members, Network Service Providers (NSPs), contracted vendors, and community partners are authorized to gain access to data information systems maintained by the network.

### ***Purpose***

This policy outlines the procedure to be followed by individuals who apply for access to a data system managed by CFBHN or the Department of Children and Families (DCF), and the technical safeguards put into place to manage that access.

### ***Procedure***

#### I. Access Request Procedures

##### A. Application Packet

1. Individuals who wish to obtain access to a network data system must complete the *CFBHN System Access Request Packet*. The packet is maintained on the CFBHN website: [www.cfbhn.org](http://www.cfbhn.org). It is found under the 'Resources' heading, and is accessed by clicking 'Agency Resources,' and 'Forms.'
2. The packet includes:
  - a. A *General Instructions* sheet, which includes the link for the applicant to access and complete two DCF web-based trainings:
    - 1) *Security Awareness*
    - 2) *HIPAA Information and Action*
  - b. A *CFBHN System Access Request* form which must be completed by the individual seeking access and signed by his or her supervisor;
  - c. A *DCF/CFBHN Security Agreement* form, to be signed by the individual seeking system access.
3. The applicant is required to complete the forms listed above, and submit them and proof of training completion to [RequestAccess@cfbhn.org](mailto:RequestAccess@cfbhn.org).
4. Once received, the packet is reviewed by the Systems Administrator for completeness, and to ensure that all required signatures are present. If a packet is incomplete, the user is notified about missing information.
5. Once the Access Request Packet is complete, the Systems Administrator enters the packet into the SharePoint Data Access list. Access packet documentation is maintained by the Information Technology (IT) department. Documentation related to CFBHN staff members' data system access is maintained by Human Resources.

##### B. Access Authorization

1. The Systems Administrator grants the appropriate access to systems managed by CFBHN.
2. Access to CFBHN and DCF data systems is granted only after it is determined that the individual requesting access:
  - a. Requires it to complete the tasks of his or her job, or

**Data System Access Management (continued)**

- b. Is doing so as specified in a formal agreement, contract and/or Business Associate Agreement (BAA) with the Network.
  3. As required by CFBHN's HIPAA Privacy and Security Officers, users who require special project data access, or are employed by organizations that are partners of the Network are required to sign a "HIPAA Guidelines for Staff of Partnering Organizations" form.
  4. Access is restricted to data networks that are appropriate to each employee's job duties. The confidentiality and integrity of data stored on CFBHN computer systems are protected by access controls to meet HIPAA requirements and ensure that only authorized employees have access to them.
  5. If access is requested for a system managed by DCF, the *System Access Request Packet and DCF form "Database Access Request"* must be completed and forwarded to the DCF staff member responsible for authorizing access. Once access is granted, the CFBHN Systems Administrator assign roles in accordance with DCF policy.
- C. Temporary Authorization
  1. When performing special software and/or hardware maintenance functions, contract personnel may be given temporary rights to the system.
    - a. The work of contract personnel is supervised by the Systems Administrator or their designee.
    - b. Business Associate Agreements (BAAs) must be in place with contracted vendors, which require them to adhere to federal and state privacy laws.
  2. User IDs that grant access are changed or disabled immediately after the contract work is completed.
- D. Deactivation
  1. CFBHN network accounts are disabled automatically after 90 days of inactivity. DCF network access locks after 45 days of inactivity and disables the account after 60 days.
    - a. If an individual's access activation packet is current, their account can be reactivated upon request.
    - b. If an individual's access activations are not current, he or she must submit a new access request packet, including current training certificates to reinstate their access.
  2. The CFBHN IT department processes all changes to user accounts upon receipt of a written request from the end user's supervisor. In the event that access to a CFBHN or DCF-managed information system is no longer required, a *CFBHN System Access Deactivation Form* must be completed and submitted to [RequestAccess@cfbhn.org](mailto:RequestAccess@cfbhn.org).
    - a. The deactivation Form can be found on the CFBHN website. It is found under the 'Resources' heading, and accessed by clicking 'Agency Resources,' and 'Forms.'
    - b. The form must be submitted to CFBHN within one (1) business day of the termination of the staff member's access.

**Data System Access Management (continued)**

II. Unique User Identification

- A. Each user is assigned a unique identifier. It includes the agency identification number assigned specifically to an organization followed by the first initial and last name of the user.
- B. Electronic mail systems employ user IDs and associated passwords to isolate the communications of each user. All CFBHN staff and authorized contractors are assigned unique user names and utilize passwords to access the email system.

III. Emergency Access Procedure

This process is documented in the *Disaster Recovery and Emergency Mode Operations* policy.

IV. Automatic Log-Off

- A. Screen locks are enabled on CFBHN-issued laptop and desktop computers, cell phones and tablets.
  - 1. Computer screen locks initiate after a 10-minute period of inactivity.
  - 2. Cell phones lock after 60 seconds of inactivity. Passwords are required at every log in.
- B. Protection settings require the user's password to be entered to regain access to the system.

V. Encryption and Decryption

- A. CFBHN electronic communications systems are not encrypted by default.
- B. If sensitive information, including protected health information (PHI) must be shared via an electronic communications system, the use of SharePoint, encryption or a technology approved by the IT department to protect the data must be utilized.
  - 1. Standard practice is to place information containing PHI into CFBHN's secure SharePoint site.
  - 2. In the event that PHI must be emailed, staff must use a zipped attachment to transmit the information with 128-bit encryption and a strong password.
  - 3. Staff are encouraged to consult with the IT staff to assist in determining the most appropriate process for the secure communication of sensitive information.
- C. An *Authorization to Release* form, signed by the individual with legal authority to make the request, must be completed to send or share client-specific PHI with others outside of CFBHN.

<p><b>Data System Access Management</b></p> <p>Approval: </p> <p>Linda McKinnon, President/Chief Executive Officer</p>	<p>Date Issued: <u>11/01/04</u></p> <p>Last Revision: <u>05/24/2021</u></p> <p>Review Date: <u>05/24/2021</u></p>
---	---