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, including but not limited to Carisk, Sharepoint, WITS, IRAS, TANF and RLDatix, must complete an Access Packet. To request these documents, a help desk ticket is submitted to Carisk. Upon completion, the forms are submitted back to Carisk for review and processing.

        2. The Access Packet includes:
            a. A 'CFBHN System Access Request' form which must be completed by the individual seeking access and signed by his or her supervisor;
            b. A 'DCF/CFBHN Security Agreement' form, to be signed by the individual seeking system access.
            c. A Data Access instruction sheet which that guidance to individuals completing the packet, and describes each of the databases to which they may request access.

        3. Once the packet is received by Carisk, it is reviewed by the Carisk 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.

        4. Once the Access Request Packet is complete, the Carisk Systems Administrator alerts the CFBHN Systems Administrator to the CFBHN-administered data systems to which the individual requires access. Access packet documentation is maintained by Carisk. Documentation related to CFBHN staff members' data system access is maintained by the CFBHN Systems Administrator.

    B. Access Authorization
        1. 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
            b. Is doing so as specified in a formal agreement, contract and/or Business Associate Agreement (BAA) with the Network.

        2. The CFBHN Systems Administrator grants the appropriate access to systems administered by CFBHN.

Data System Access Management (continued)

3. Carisk is responsible for working with the Department to grant access to an individual who requests access to a DCF-managed data system.

4. 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.

5. 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.

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. In the event that access to a CFBHN or DCF-managed information system is no longer required, a 'System Access Deactivation' form must be completed and submitted to Carisk.
      a. If a staff member's employment with CFBHN is terminated:
         1) The HR Manager immediately alerts Carisk by submitting a Help Desk ticket. The Help Desk ticket must:
            a) Identify the individual who no longer requires access;
            b) Include the date that access should be discontinued; and
            c) Be submitted to Carisk within twenty-four hours of the change to the staff member's required access.
         2) Carisk will provide the HR Manager with a 'System Access Deactivation' form. The HR Manager will forward the form to the CFBHN Senior Systems Administrator to complete and return to Carisk.
      b. If a staff member remains employed with CFBHN, but changes in responsibilities or job duties no longer require access to a particular CFBHN or DCF data system, the staff member's direct supervisor is responsible for submitting a Help Desk ticket to Carisk and completing a 'System Access Deactivation' form.

   2. Once complete, the Deactivation form is maintained by Carisk, and formally documents the written request for a change in the user's access from the user's supervisor.

   3. 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.

Data System Access Management (continued)

      a. If an individual's access activation packet is current, and reactivation is required, their account can be reactivated upon request.

      b. If an individual's access activations are <u>not</u> current, he or she must submit a new access request packet, including current training certificates to reinstate their access.

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 usernames 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 15 seconds of inactivity. Authentications are required at every log in.

    B. Protection settings require the user's biometrics/password/authentication application and/or multi-factor authentication to be provided 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.

Data System Access Management Approval: Alan Davidson, President/Chief Executive Officer	Date Issued: <u>11/01/2004</u> Last Revision: <u>09/11/2024</u> Review Date: <u>09/11/2024</u>