Confidentiality of Individuals Served/Minimum Necessary Requirements

Policy

It is the policy of Central Florida Behavioral Health Network, Inc. (CFBHN) to comply with federal and state laws related to the confidentiality of individuals served, and the protection of their health information. This includes, but is not limited to, defined statutes related to the Health Insurance Portability and Accountability Act (HIPAA, 45 CFR Part 160-164), 42 CFR Part 2, 397.501(7) F.S., and 394.4615 F.S.

Purpose

The purpose of this policy is to outline CFBHN policies and procedures regarding the confidentiality of individuals served, and to limit unnecessary or inappropriate access to, and disclosure of, their protected health information (PHI).

Procedure

A. Confidentiality Guidelines for CFBHN Staff Members

1. All CFBHN employees are expected to abide by the provisions of federal and state laws related to the confidentiality of individuals served and the protection of their health information. As defined in the *HIPAA Sanctions* policy, failure to do so may result in disciplinary action, up to and including, termination.

2. At hire, and on an annual basis thereafter, CFBHN employees complete HIPAA privacy and data security awareness trainings. Completion of training is required for staff members to initiate or maintain access to the Network's Information Technology (IT) and data systems. Training documentation is maintained through the MyFLLearn system.

3. Staff are required to adhere to HIPAA privacy and security guidelines while working in the office, or remotely from their home or field location. On an annual basis, employees are required to sign the *Privacy, Security and Risk Mitigation Guidelines for Staff Working Remotely* form. This document is maintained in each employee's personnel file.

4. Staff members are not permitted to share their passwords with others. Passwords must be kept secure at all times.

5. Staff are not permitted to make any changes to security or administrative settings on CFBHN-issued equipment.

6. Only CFBHN employees are permitted to use CFBHN-issued equipment. Others, including family members, are not permitted to use equipment that is the property of CFBHN.

7. Staff may use personal devices to access email through Outlook Web Access (OWA), but are not allowed to download CFBHN-related data onto those devices. CFBHN-related data is defined as, but not limited to, network billing and service data, reports, personnel records, identifying information, and protected health information (PHI).

8. Texting of identifying information or PHI is not permitted.

9. Staff must use the Net Extender VPN to access CFBHN data systems while working off site.

Confidentiality of Individuals Served/Minimum Necessary Requirements (continued)

10. Staff must position workstations and computer screens out of the sight of others to prevent the unauthorized view of identifying information, PHI, and/or other sensitive data.

11. Staff must close and log out of programs containing identifying information, PHI, or other sensitive data when they are not in use. Staff must lock, log out, or shut down the computer before walking away from the device.

12. Microsoft Teams, or another HIPAA-compliant platform, must be used to conduct teleconferencing sessions that include identifying information or PHI.

13. Phone or teleconferencing discussions that involve identifying information, PHI, or other sensitive data, must be held in a private setting. A private setting is defined as an area that is not accessible by, or in earshot of, members of the public, family members, visitors to the office/remote work locations, or other individuals who are not involved in the meeting or conversation.

14. Staff access to personal information and/or PHI of individuals served is determined by the responsibilities of their job duties at CFBHN. Two levels of data access are identified:
    A. FULL access applies to CFBHN positions with job responsibilities that involve contract oversight, finance and program compliance monitoring, utilization management, care coordination, program management, quality improvement activities, and incident investigation. These positions require full access to the data shared with CFBHN by its Network Service Providers (NSPs):
        1) President/Chief Executive Officer (CEO), Chief Operating Officer (COO), Chief Financial Officer (CFO), Vice President of Network Development and Clinical Services (NDCS).
        2) Continuous Quality Improvement (CQI) Director, Manager and Quality Specialists
        3) Risk Manager and Risk Specialist
        4) Clinical Program Specialists, Behavioral Health Utilization/Care Managers, Program Managers, Community Managers, Consumer and Family Affairs Staff
        5) Director of Contracts, Senior Contract Managers, and Contract Specialists
        6) IT staff
        7) Accountant and Fiscal Coordinators

    B. LIMITED access permissions apply to CFBHN position with job responsibilities that involve incidental contact with PHI, including data entry, billing, typing, and correspondence. These activities may require the review of a subset of patients' PHI to ensure data accuracy. This includes the following positions:
        1) Human Resources Business Partner and/or Consultant
        2) Facilities Manager/Executive Assistant
        3) Administrative Assistants

15. Staff are not permitted to share personal or identifying information, PHI, or other sensitive individuals served data with others. This includes co-workers who do not require the information to do their job.

16. Identifying information and PHI must be encrypted or password-protected before it is sent electronically outside of the organization.

Confidentiality of Persons Served/Minimum Necessary Requirements (continued)

17. Staff are required to report unprotected identifying information or PHI sent to them from someone outside of CFBHN. They must also make a report when unprotected data is sent by them to someone outside of CFBHN. The report must be made to the Risk Management department by creating an internal incident in the RLDatix system.

18. To the extent possible, staff should avoid printing hard copies of data reports that contain identifying information, PHI, and/or other sensitive data while working off site. If printing is necessary, the document must be edited to remove or limit sensitive data, identifying information, and/or PHI to the minimum necessary.

19. Hard copies of documents that contain identifying information, PHI, or other sensitive data must be secured in a manner that protects them from access by unauthorized individuals.
    A) This type of data must be stored in a locked file cabinet, case, or drawer.
    B) Staff must use a locked case to transport hard copies of sensitive information or data reports that contain identifying information or PHI. Staff are not permitted to leave a locked case that contains sensitive data, identifying information, or PHI in a car overnight or for extended periods of time. Locked cases that contain protected data must be secured in the car's trunk for short stops during a commute.
    C) Staff must use a shredder to destroy data reports, identifying information, or PHI that is no longer needed. Use of cross-cut shredders is the preferred method of destroying documents. Hard copies that include PHI may also be placed into the secure, locked bins located at the CFBHN office.

20. Staff must immediately alert the IT department if access to a CFBHN database or data source is no longer required.

21. Staff must report any privacy and/or security issues to their supervisor, and CFBHN's HIPAA Privacy and Security Officers.

B. Treatment Records Requests
    1. Requests for treatment records of individuals served require the completion of an *Authorization to Release* form, signed by the individual served their guardian or legal representative.
        A) Authorization for release requests may be made electronically or in writing. Copies of all disclosure requests and completed authorization forms are kept on file by CFBHN.
        B) Verbal authorizations are not accepted.
        C) This type of request is managed by the Executive Assistant, Vice President of NDCS or the Privacy Officer. (Please also see CFBHN's *'Authorization to Release Client Information'* policy.)

    2. Subpoenas, court orders, search warrants, investigations, and any other CFBHN-related legal requests are handled by the Chief Operating Officer and/or Human Resources. (Please also see CFBHN's *'Subpoenas, Court Orders, and other Legal Matters'* policy.)

    3. As applicable, staff members must follow the HIPAA 'Minimum Necessary' requirements outlined in Section D of this policy.

Confidentiality of Individuals Served/Minimum Necessary Requirements (continued)

C. Confidentiality Requirements for Network Service Providers (NSPs)

1. Each NSP is responsible for the development, implementation, and maintenance of policies and procedures that meet applicable regulatory, licensure, and accreditation standards related to individuals served records and the release of protected health information (PHI). NSPs are required to ensure their staff are aware of, and comply with, these standards.

2. CFBHN enters into a Business Associate Agreement with each NSP and business entities involved within the network, to maintain compliance with confidentiality requirements and required health information protections.

D. HIPAA 'Minimum Necessary' Requirements

1. The HIPAA Privacy rule requires covered entities to take reasonable steps to limit the use or disclosure of, and requests for, PHI to the minimum necessary to accomplish the intended purpose.

2. CFBHN evaluates each request on an individual, case-by-case basis to ensure the disclosure includes only the minimum amount of information that is needed. This is permitted by the Privacy Rule when the request is made by:
   a. Another covered entity;
   b. A researcher with appropriate documentation from an Institutional Review Board (IRB) or Privacy Board;
   c. A public official or agency that states that the information requested is the minimum necessary for a purpose permitted under 45 CFR 164.512 of the Rule, such as for public health purposes (45 CFR 164.512(b)).

3. The minimum necessary standard does not apply in the following instances:
   a. Disclosures to, or requests by, a health care provider for treatment purposes.
   b. Disclosures to the individual who is the subject of the information.
   c. Uses or disclosures made pursuant to an individual's authorization.
   d. Uses or disclosures required for compliance with the HIPAA Administrative Simplification Rules.
   e. Disclosures to the Department of Health and Human Services (HHS) when disclosure of information is required under the Privacy Rule for enforcement purposes.
   f. Uses or disclosures that are required by other law.

Confidentiality of Individuals Served/Minimum Necessary Approval: Alan Davison, President/Chief Executive Officer	Date Issued: 11/01/2002 Last Revision: 08/28/2024 Review Date: 08/28/2024