Information Technology (IT) Security Responsibilities

Policy
It is the policy of Central Florida Behavioral Health Network, Inc. (CFBHN) to document staff responsibilities related to security measures specified by the Health Insurance Portability and Accountability Act (HIPAA) and state statutes.

Purpose
The purpose of this policy is to define staff responsibilities related to IT security.

Procedure
I. Primary Responsibilities
   A. CFBHN's Chief Operating Officer (COO) and the CFBHN Senior Systems Administrator oversee organization-wide IT and computer systems and are responsible for establishing policies to protect security of hardware, software, and data.

   B. HIPAA Officers
      1. Security Officer
         a. The COO serves as the CFBHN Security Officer. The HIPAA Security Officer is responsible for the continuous management of IT security policies, procedures, and technical systems in order to maintain the confidentiality, integrity, and availability of all organization data and information systems.

         b. Responsibilities of this position include, but are not limited to:
            1) The development of appropriate policies and procedures related to IT security and the protection of health information.
            2) IT security practice compliance and the enforcement of sanctions for staff and Business Associates that do not comply.
            3) Development of standards that govern access to protected health information (PHI).
            4) Delivery of security training for new CFBHN staff and Business Associates.

      2. Privacy Officer
         a. The Director of Continuous Quality Improvement (CQI) serves as the CFBHN Privacy Officer. The HIPAA Privacy Officer oversees the development, implementation, and adherence to privacy policies and procedures regarding the safe use and handling of PHI.

         b. Responsibilities of this position include:
            1) Development and maintenance of appropriate privacy/confidentiality consents, authorizations, and notices in accordance with CFBHN policies and regulatory requirements.
            2) Ensure that all employees complete privacy training at orientation and at regular intervals thereafter.
            3) Track, document, investigate, and act on complaints related to privacy policies/ procedures.

   C. Both the Security Officer and Privacy Officer are responsible for:
      1. Ensuring that periodic risk assessments and related compliance monitoring initiatives are completed.

Information Technology (IT) Security Responsibilities (continued)

2. Working with the Director of Contracts and Procurement, ensuring that Business Associate Agreements are current, and Business Associates maintain compliance with privacy and security requirements.

3. Training staff on compliance with privacy and security policies and procedures.

4. Maintaining up-to-date knowledge of privacy laws and HIPAA regulations to ensure organizational compliance.

II. Other Positions and Defined Responsibilities

A. Chief Operating Officer (COO):
   a. Supervises the work of the HIPAA Privacy Officer.
   b. Conducts an annual risk assessment of information systems utilized by CFBHN. The purpose of this assessment is to identify areas of vulnerability, and to develop a plan to mitigate risks of identified weaknesses.

B. IT Senior Systems Administrator
   a. Monitors compliance with internet security requirements, including hardware, software, and data safeguards and reports any issues to the COO.
   b. Provides administrative support and technical guidance to management on matters related to IT security.
   c. Reviews and approves data system access requests made by CFBHN staff and employees of Network Service Providers (NSPs). This includes that guidelines related to role-based access are met.

C. Contracted Vendors of IT Services
   1. Lightwave Management Resources
      a. CFBHN contracts with Lightwave to provide IT consulting services, and assistance with the CFBHN phone system and systems migrations.
      b. Lightwave staff work closely with the Senior Systems Administrator, and serve as his backup, as required, to provide technical assistance and guidance to staff.

   2. Carisk Partners
      a. CFBHN contracts with Carisk to utilize its data and billing system.
      b. Carisk administrators are responsible for managing the security of system, and assist with granting access to Carisk, DCF, and CFBHN data systems utilized by CFBHN and NSP staff.

   3. RLDatix
      a. CFBHN contracts with RLDatix for access to its Risk Management software.
      b. RLDatix administrators are responsible for the protection and security of data contained within that system.
      c. CFBHN staff are responsible for issuing licenses and granting access to the RLDatix system.

   4. JRP Global manages the front and back-end of the CFBHN website.

Information Technology (IT) Security Responsibilities (continued)

D. CFBHN Managers and Directors:

1. Approve requests for access to data systems maintained by CFBHN. This includes ensuring that the staff member has access only to the data systems necessary to complete the tasks of his or her job responsibilities.

2. Initiate the data access deactivation process upon a staff member's termination of employment, or if their position no longer requires access to a particular data system.

3. Work with the HIPAA Privacy and Security Officers to establish data-sharing agreements between CFBHN and community partners that involve client-specific data and/or PHI.

4. Ensure that staff under their supervision are actively adhering to privacy and security standards established by CFBHN policy and federal/state regulation. This includes the enforcement of sanctions against staff who violate established procedures and guidelines.

Information Technology (IT) Security Responsibilities Approval: Alan Davidson, President/Chief Executive Officer	Date Issued: 10/01/2003 Last Revision: 04/28/2023 Review Date: 07/31/2024