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 Director of IT oversee organization-wide computer systems and are responsible for establishing policy to protect security of hardware, software and data.

B. HIPAA Officers

1. Security Officer

a. The Director of IT 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 personal 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, 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. Performing periodic risk assessments and related compliance monitoring initiatives.
2. Ensuring that Business Associate Agreements are current, and Business Associates maintain compliance with privacy and security requirements.

Information Technology (IT) Security Responsibilities (continued)

3. Ensuring that staff are acting in 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 of Responsibility

A. Chief Operating Officer (COO): The COO supervises the work of the HIPAA Privacy and Security Officers.

B. IT System Administrator

1. Monitors compliance with internet security requirements, including hardware, software, and data safeguards and reports any issues to the CFBHN IT Director. The System Administrator also provides administrative support and technical guidance to management on matters related to IT security.

2. 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.

3. Conducts an annual risk assessment of each production information system. The position is responsible for determining both risks and vulnerabilities, and reports any issues to the CFBHN IT Director.

C. CFBHN Managers and Directors:

1. Approve requests for access to data system 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.

Assigned Information Technology (IT) Security Responsibilities Approval: Linda McKinnon Linda McKinnon, President/Chief Executive Officer	Date Issued: 10/01/03 Last Revision: 04/06/2021 Review Date:04/06/2021