Central Florida Behavioral Health Network, Inc.
Your Managing Entity

Information Technology Plan

FY 25-26

FLORIDA DEPARTMENT OF CHILDREN AND FAMILIES
MYFLFAMILIES.COM

Revised: 08/28/2025
Approved by Risk Management/CQI Oversight Committee:08/28/2025
Submitted to DCF: 08/29/2025

Administrative Office
719 South US Highway 301
Tampa, FL 33619
813.740.4811
www.cfbhn.org

OVERVIEW

This plan summarizes the work of the Central Florida Behavioral Health Network (CFBHN) Information Technology (IT) department. IT is an essential tool that allows CFBHN to streamline financial transactions, increase staff efficiency, decrease administrative costs, communicate with stakeholders, and maintain reliable accessible data collection and reporting. Each of these activities also allows CFBHN to gather the data needed on which to base funding decisions and carry out the goals established in the Network's strategic plan. The mission of the IT department is to support the strategic business and operational objectives of CFBHN through innovative customer-oriented systems and technologies. The Information Technology Plan is reviewed and updated on an annual basis.

IT DEPARTMENT ACTIVITIES

The IT Department is managed by the Chief Operating Officer (COO) and the CFBHN IT Department Staff. This work is supported by Lightwave Management Resources, an external company with which CFBHN subcontracts to act as a support system for CFBHN's internal IT Support Team, and to provide repairs and/or updates to CFBHN's internal network. The CFBHN Senior Systems Administrator, CFBHN Systems Support Analyst and Lightwave Management Resources oversee daily operation of the internal and external data systems, and assist users with training, support, and technical assistance. IT uses all forms of communication when supporting Network Service Providers (NSPs) funded by CFBHN. This includes, but is not limited to, a helpdesk ticket system, email, fax, telephone, Microsoft Teams and ZOHO (Remote Assist).

Management of the CFBHN data system is outsourced to Carisk Partners. CFBHN and Carisk Partners work in partnership to meet the requirements of the DCF, and other contract funders, on the submission and analysis of data, CFBHN uses the Carisk Partners platform for contract data management, invoicing management, CFBHN's electronic waitlist, and a Coordination of Care module.

Carisk Partners plays an integral role in the Information Technology Plan for CFBHN as it relates to provider, client-specific and service data. Principally, Carisk Partners develops and maintains a bespoke online portal and database system utilized by CFBHN and its NSPs. Demographic, performance, clinical, financial, and service data is submitted to this portal by NSPs, maintained in a secure database by Carisk Partners, and submitted to DCF according to the requirements in DCF's pamphlet 155-2 (FASAMS), the stipulated General Appropriations Act (GAA), and National Outcome Measures (NOMs). Both Network Service Providers and CFBHN further utilize the portal to evaluate data quality in real time, track performance measures, evaluate utilization and effectiveness of services, and fully manage and process invoicing. Carisk Partners administers the database and access to the portal in accordance with HIPAA and DCF security standards.

In addition to comprehensive report-building capabilities, the Carisk Partners portal has a set of tools which leverage provider, contractual, demographic, admissions, discharge, performance and service event data in its database to enable programmatic, financial, clinical, and data quality analysis at the network, provider, and individual client levels. Various dashboards provide real-time visibility to provider utilization of services, missing data, performance measures, numbers served and the ability to see a client's episode of care from beginning to end. The online application also captures trends within the network focused on provider performance.

All Carisk Partners systems are hosted in a secure data hosting facility. Access to provider and client data is restricted to authorized personnel and through multiple security levels. Carisk Partners has strict information security, confidentiality and quality improvement policies and procedures for the entry and protection of data for individuals served and providers.

Department staff work with CFBHN leadership and the CFBHN Board of Directors as needed, to formulate strategic direction, and develop policy to enhance the operation and efficiency of the Network's data systems.

NETWORK SECURITY

Data security is maintained in accordance with the Health Insurance Portability and Accountability Act (HIPAA) guidelines, 42 CFR, Part 2, state law, and policies and procedures established by DCF and CFBHN. CFBHN's hardware and data network are designed and maintained in accordance with the security standards established by policy and statute. CFBHN's data security policies are reviewed on an annual basis and are available for review upon request.

The current hardware configuration consists of a multi-server network behind a secure multi-layer firewall located in Tampa. External providers link with the system via a secure connection. CFBHN's data is co-located at Flexential to allow the Network to protect and recover data in the event of an emergency or natural disaster. Flexential is ISO 27001:2013 certified data center, providing a fault-tolerant secure environment. The facility is located in a non-hurricane evacuation zone and on the airport grid. Flexential is located at 9417 Corporate Lake Drive, Tampa, FL.

SOFTWARE TECHNOLOGY AND REPORTING

The information management systems utilized by CFBHN are listed below.

- Carisk Partners

  CFBHN utilizes the Carisk Partners system to collect, track and trend service data. The system is also utilized for billing and invoicing, contract management and includes the following features:

  - Registration of individuals served
  - Screening and assessment summaries of registered individuals
  - Service tracking for individuals served, including intakes, admissions, discharges, and follow-up
  - Submission and approval of service voucher requests
  - Identification of 'High Need-High Utilizer' clients and eligibility for Care Coordination
  - Service waitlist tracking
  - File processing of FASAMS data

  CFBHN works directly with Carisk Partners to develop and customize additional features of the platform, as needed.

- Microsoft SharePoint

  This system allows approved users to exchange data securely, in a privilege-based environment, and tracks all transactions. SharePoint is utilized by all CFBHN departments to safely share documents with NSPs and vice versa. It is also used by CFBHN and NSP staff to submit and store documents required by contract.

- RLDatix

  RLDatix was introduced in 2016 to allow CFBHN's Risk Management department to more efficiently manage its incident report data. The system is utilized by approved users from each of the network's NSPs to report critical incidents that occur at their sites, and that impact their clients. RLDatix includes an automated report system that summarizes the number of reports made by each NSP monthly, and a 'task' function that allows CFBHN staff to communicate directly with NSPs with questions and/or document requests. RLDatix is also utilized by CFBHN to track internal incidents and events, defined as actions that involve the release of information or a report to a third-party and are required to be documented or tracked. Access to this platform is maintained through a contract with the software designer.

DATA REPORTING CAPABILITIES

CFBHN's reporting systems are continually developed and enhanced to include the export of data sets from the information management systems, the production and distribution of custom reports, and granting data access to internal and external staff. CFBHN's IT Support Team, with input from the management team, NSPs and stakeholders, produce standardized reports on key measures for each contract. A hub of standard reports, accessible by all CFBHN staff, is also available on SharePoint and with Carisk Partners.

Internal monthly reports analyze the performance of the NSPs funded by CFBHN and assist with the tracking of contract requirements. Through dashboard reports that summarize service targets established by the Department of Children and Families (DCF), CFBHN is able to track the performance of each individual NSP, and that of the Network as a whole.

STRATEGIC GOALS, OBJECTIVES AND PRIORITIES

The goals, objectives and priorities of the CFBHN IT department for FY 25-26 are summarized below.

Short-Term Goals (Timeframe: Completion within 1 to 6 months)

1. **Work with Carisk Partners for the implementation of the Encounter Notification System (ENS) by the end of FY 25/26.**

   Priorities:
   a. Develop a data collection method for population identified to utilize the ENS system.
   b. Work alongside Carisk Partners for the notification to be embedded within the Carisk system.

   Technology acquisition, maintenance or replacement required: CFBHN would have to enter into an agreement with ENS as an ENS subscriber.

   Resources required: Staff time

Intermediate Goals (Timeframe: Completion within 6 to 12 months)

2. **Continue the implementation of the DCF Financial and Services Accountability Management System (FASAMS V14), and the associated changes to CFBHN systems.**

   Priorities:
   a. Mitigate impacts to NSP billing as data issues are identified and corrected.
   b. Maintain open communications with NSPs over the course of the data system transition.
   c. Work to ensure that data reports are available, as needed, by CFBHN staff and stakeholders during the data system transition.

   Technology acquisition, maintenance or replacement required: No need for new technology is anticipated at this time. Existing technology will address these goals.

   Resources required: Staffing and staff time

3. **Evaluate IT security risks and implement strategies to mitigate identified vulnerabilities**

   Priorities:
   a. Implement a security strategy from the Security Risk Assessment Toolkit.
   b. Perform internal security review using Symantec, MS Defender, and firewall logs. Bring Webapp/Website vulnerability testing in-house. Continue to design helpful and workforce targeted Phish

testing campaigns using KnowBe4 and implement end user education resulting in improved testing performance.

Technology acquisition, maintenance or replacement required: Based on the solutions identified, new technology will not be required.

Resources required: Staff time

Long-Term Goals (Timeframe: Completion within 1 to 3 years)

4. Align CFBHN's systems and functionality more closely with those utilized by other Managing Entities

Priorities:

a. Utilize current Microsoft Cloud technology for enhanced collaboration and security.
b. Move all business-critical resources to data center and cloud for maximum availability and reduce any risk that may exist due to on-prem equipment.
c. Continue to leverage licensing by using Business to Business (B2B) for all users who have a Microsoft 365 account.

Technology acquisition, maintenance or replacement required: Based on the solutions identified, new technology will not be required.

Resources required: Staff time

5. Continue to develop IT infrastructure to enhance reporting ability.

Priorities: Timely and accurate reporting

Technology acquisition, maintenance or replacement required: Based on the solutions identified, new technology will not be required.

Resources required: Internal staff and external contractors will handle the execution of these goals.

PROGRESS ON PREVIOUS YEAR'S GOALS - FY 24-25

Short-Term Goals (Timeframe: Completion within 1 to 6 months)

1. Working directly with Carisk Partners, complete projects identified on the 'Priority List' to continue to customize the platform to meet CFBHN needs.

Priorities:

a. Maintain an accurate list of priority projects. This list is updated on a regular basis by the Director of Contracts.
b. Continue to meet weekly with Carisk Partners staff to communicate directly on 'Priority List' progress.

Progress Summary: Fifteen (15) items on the priority list were completed during FY 24/25. Weekly meetings with Carisk Partners are held throughout the year to continue to address data needs identified as priorities.

Intermediate Goals (Timeframe: Completion within 6 to 12 months)

2. Continue the implementation of the DCF Financial and Services Accountability Management System (FASAMS V14), and the associated changes to CFBHN systems.

Priorities:

a. Mitigate impacts to NSP billing as data issues are identified and corrected.
b. Maintain open communications with NSPs over the course of the data system transition.
c. Work to ensure that data reports are available, as needed, by CFBHN staff and stakeholders during the data system transition.

Progress Summary: CFBHN continued with work with Carisk Partners and NSPs on the associated changes within FASAMs. CFBHN continues to identify reports to be developed by Carisk to ensure accurate and timely data submission to DCF.

3. Evaluate IT security risks and implement strategies to mitigate identified vulnerabilities

Priorities:
a. Complete Internal Security Risk Assessment
b. Develop strategies to mitigate identified vulnerabilities from Internal Security Risk Assessment
c. Select a vendor for external Penetration Testing
d. Evaluate the use of external phish testing/education for CFBHN employees

Progress Summary: An internal security risk assessment was completed FY 24/25. Vulnerabilities were identified and strategies were implemented to help mitigate identified risks. A vendor was selected and DataComm completed the external penetration testing. KnowB4 was implemented for employee phish testing and training.

Long-Term Goals (Timeframe: Completion within 1 to 3 years)

4. Align CFBHN's systems and functionality more closely with those utilized by other Managing Entities.

Priorities: Cloud computing and virtualization solutions are the top priorities.

Progress Summary: CFBHN has made progress with moving additional data resources from CFBHN system over to Carisk Partners.

5. Re-design existing data structures and IT infrastructure to utilize emerging technologies that will enhance reporting ability.

Priorities: Cloud computing and virtualization solutions are the top priorities.

Progress Summary: Progress on these goals continues.