

---

## Business Associate Agreements

### ***Policy***

It is the policy of the Central Florida Behavioral Health Network, Inc. (CFBHN) to maintain Business Associate Agreements (BAAs) with Network Service Providers (NSPs), contracted vendors, and network partners that access data systems or physical space, and/or with which Protected Health Information (PHI) or electronic Protected Health Information (ePHI) is shared.

### ***Purpose***


The policy outlines compliance measures established as components of CFBHN's BAAs.

### ***Procedure***

- I. Business Associate Agreements
  - A. CFBHN requires each NSP, contracted vendor, and/or network partner with which PHI is created, received, maintained, transmitted or shared to sign a CFBHN BAA. This includes those that access data systems or physical space at the CFBHN office.
  - B. The BAA specifies the terms of the data exchange between CFBHN and the third party, as well as expectations as to how client identifiers and health information are handled and protected.
  - C. The BAA must be signed by the NSP or vendor's Chief Executive Officer, or other administrator with signing authority, and returned to CFBHN prior to the execution of the contract or agreement.
  - D. The BAA must be signed by CFBHN and the second party prior to the initiation of the data exchange, or access to data systems or facility space is given.
  - E. Active BAAs are maintained by the Contracts department, and updated as necessary.
  - F. The need for a BAA is evaluated based on the nature of the purchase agreement or purchase order.
- II. HIPAA Compliance
  - A. As noted in contract, Business Associates contracted with CFBHN agree to comply with all applicable requirements of HIPAA Privacy and Security regulations, including, but not limited to requirements to:
    1. Maintain current HIPAA policies and procedures.
    2. Appoint a HIPAA Privacy and Security Officer.
    3. Conduct staff security awareness training at hire, and at regular intervals and/or when training updates are needed. This includes completion of the Department of Children and Families (DCF) HIPAA training required annually of NSPs with access to CFBHN data systems.
    4. Conduct risk analysis, and adhere to contract, state, and federal notification requirements in the event of a breach of PHI.
    5. Maintain BAAs with organizations with which they subcontract to create, receive, maintain, or store health information.
  - B. CFBHN Business Associates and their contractors are not permitted to use or disclose PHI/ePHI other than as allowed or required by contract or federal and state law.
  - C. Business Associates and/or their subcontractor(s) are directly liable under the civil and criminal enforcement provisions for failure to comply with HIPAA Rules and any guidance issued by the Secretary of Health and Human Services.

**Business Associate Agreements** (continued)

- D. Business Associates are required to adhere to the breach notification requirements defined in 45 CFR § 164.410, and to notify CFBHN upon discovery of a breach that compromises the privacy and security of unsecured PHI/ePHI.
    - 1) A Business Associate must provide notice to CFBHN and DCF without unreasonable delay and no later than 60 days from the discovery of the breach.
    - 2) As necessary, and to the extent possible, the Business Associate must provide DCF with information on the breach. In the event of a breach or possible breach, the Business Associate is asked to complete DCF documentation for review by the Department’s Security Officer.
  - E. In the event of an impermissible use or disclosure of PHI, Business Associates must demonstrate and maintain documentation that all required notifications were made or, alternatively, that notification was not required because (1) its risk assessment demonstrated a low probability that the PHI/ePHI had been compromised, or (2) the use or disclosure of PHI/ePHI met any of the exceptions to the definition of a formal breach.
  - F. At its discretion, CFBHN will suspend or terminate Business Associate and NSP user access to CFBHN systems, issue letters of correction, and/or require the submission of a corrective action plan related to any potential or known concern regarding the security of PHI/ePHI.
  - G. Through its Risk Management department, CFBHN notifies its Business Associates and/or involved staff members when the Network becomes aware of the use or disclosure of PHI/ePHI. This process includes the completion of a risk assessment to determine the likelihood that an unauthorized disclosure of PHI or ePHI has taken place.
- III. HIPAA Compliance Monitoring
- A. BAAs are maintained by the CFBHN Contracts department.
  - B. Carisk, Lightwave and CFBHN’s Information Technology department share responsibility for all user access to network data systems.
  - C. NSP compliance with the terms of this policy are monitored by the CQI department during annual reviews of each organization. Reviews include verification that:
    - 1. Each NSP has appointed a formal Privacy and Security Officer.
    - 2. HIPAA policies and procedures have been developed by the organization.
    - 3. Staff training on HIPAA policies and procedures occurs at the time of hire and at regular intervals thereafter.
    - 4. When a user no longer requires access to a network data system, Carisk is notified within 24 hours of this change.

<p><b>Business Associate Agreements</b></p> <p>Approval:  Alan Davidson, President/Chief Executive Officer</p>	<p>Date Issued: <u>04/01/2003</u></p> <p>Last Revision: <u>07/25/2023</u></p> <p>Review Date: <u>07/25/2023</u></p>
---	---