Business Associate Agreements

Policy

It is the policy of the Central Florida Behavioral Health Network, Inc. (CFBHN) to evaluate each Network Service Provider (NSP), vendor, contractor, consultant, network partner, technology provider, and other third-party relationship to determine the parties' potential risks, appropriate HIPAA roles and monitoring, and applicable agreement requirements, including communications protocols.

NSPs generally function as Covered Entities with respect to PHI/ePHI they create, receive, maintain, or transmit in furnishing health care services. CFBHN may function as a Business Associate when it creates, receives, maintains, transmits, accesses, uses, or discloses PHI/ePHI on behalf of a provider or other Covered Entity.

Outside vendors, contractors, consultants, technology providers, and other third parties may function as Business Associates or subcontractor Business Associates when they create, receive, maintain, transmit, access, support, host, troubleshoot, or otherwise have the ability to access PHI/ePHI through CFBHN systems, data systems, applications, records, services, or physical space.

CFBHN requires appropriate written BAA provisions or agreements to be in place before PHI/ePHI is accessed, exchanged, created, received, maintained, transmitted, used, or disclosed, unless a documented and justified exception applies.

Purpose

The policy is to establish CFBHN's process for determining HIPAA roles, documenting the required Business Associate Agreement (BAA) provisions, managing CFBHN's obligations when acting as a Business Associate, and ensuring that vendors or downstream subcontractors with access to PHI/ePHI provide appropriate written assurances and comply with applicable privacy, security, breach notification, and access requirements.

This policy shall be construed liberally to comply with all applicable HIPAA and 42 CFR Part 2 requirements, and as amended by law or rule.

I Definitions

A. **Covered Entity** – a health plan, health care clearinghouse, or health care provider that conducts covered electronic transactions under HIPAA. For purposes of this policy, NSPs and other provider entities generally function as Covered Entities with respect to PHI/ePHI they create, receive, maintain, or transmit in furnishing health care services.

B. **Business Associate** – a person or entity, other than a workforce member, that creates, receives, maintains, transmits, accesses, uses, or discloses PHI/ePHI to perform a function, activity, or service for or on behalf of a Covered Entity. CFBHN may function as a Business Associate when it performs network administration, reporting, coordination, quality, oversight, data, access management, or other services involving PHI/ePHI on behalf of a provider or other Covered Entity.

C. Subcontractor Business Associate – a person or entity that creates, receives, maintains, transmits, accesses, supports, hosts, processes, stores, troubleshoots, or otherwise has the ability to access PHI/ePHI on behalf of a Business Associate. A subcontractor Business Associate must provide written assurances that it will comply with the same applicable restrictions, conditions, and requirements that apply to the Business Associate with respect to PHI/ePHI.

Business Associate Agreements (continued)

D. Non-Business Associate Vendor - a vendor, contractor, consultant, or other third party that provides goods or services to CFBHN but does not create, receive, maintain, transmit, access, use, disclose, support, host, troubleshoot, or otherwise have the ability to access PHI/ePHI. A BAA is not required for a non-Business Associate vendor, although CFBHN may require confidentiality, security, access restriction, or other contractual protections as appropriate.

Procedure

I. HIPAA Role Determination and Agreement Requirements

A. Role Determination

1. CFBHN evaluates each relationship involving NSPs, vendors, contractors, consultants, technology providers, network partners, and other third parties to determine whether the party is acting as a Covered Entity, Business Associate, subcontractor Business Associate, or non-Business Associate vendor.
2. The role determination is based on the function performed, the direction of services, the applicable contract or agreement, the nature of the PHI/ePHI involved, and whether the party creates, receives, maintains, transmits, accesses, uses, discloses, supports, hosts, troubleshoots, stores, processes, or otherwise has the ability to access PHI/ePHI.
3. For purposes of this policy, access to PHI/ePHI includes creating, receiving, maintaining, transmitting, accessing, using, disclosing, supporting, hosting, troubleshooting, storing, processing, or otherwise having the ability to access PHI/ePHI.
4. A party's HIPAA role is determined by the relationship, function, and data flow. The fact that a party does not generate PHI/ePHI does not prevent it from being a Business Associate or subcontractor Business Associate if it has access to, maintains, transmits, supports, hosts, troubleshoots, or otherwise has the ability to access PHI/ePHI.

B. Network Service Providers

1. NSPs function as Covered Entities with respect to PHI/ePHI they create, receive, maintain, or transmit in furnishing health care services.
2. CFBHN may function as a Business Associate when it performs functions or services involving PHI/ePHI on behalf of such NSPs.
3. For NSP relationships, required BAA provisions are incorporated into the NSP's subcontract.
4. A standalone Business Associate Agreement is not required unless requested by the provider, required by the contracting process, or determined necessary by CFBHN.

C. CFBHN as Business Associate

1. When CFBHN acts as a Business Associate, CFBHN will use or disclose PHI/ePHI only as permitted or required by the applicable agreement, HIPAA, state law, Department of Children and Families (DCF) requirements, or other governing authority.
2. CFBHN complies with applicable privacy, security, breach notification, subcontractor, access, amendment, accounting, return, destruction, and termination obligations required by the applicable agreement and law.

Business Associate Agreements (continued)

D. Vendors, Contractors, and Other Third Parties

1. Outside vendors, contractors, consultants, technology providers, and other third parties may function as Business Associates or subcontractor Business Associates when they create, receive, maintain, transmit, access, support, host, troubleshoot, store, process, or otherwise have the ability to access PHI/ePHI through CFBHN systems, data systems, applications, records, services, physical space, or other arrangements.
2. A vendor, contractor, consultant, technology provider, or other third party may qualify as a Business Associate or subcontractor Business Associate even if it does not generate the PHI/ePHI.
3. A Business Associate Agreement is not required solely because a party is a vendor, contractor, consultant, or service provider. If the party does not have access to or the ability to access PHI/ePHI, the party is not required to execute a BAA.
4. CFBHN may still require confidentiality, data security, access restriction, or other contractual protections for Non-Business Associate Vendors, as appropriate.
5. Contracts will maintain a copy of the executed BAAs in the SharePoint folder for the vendor, contractor, consultant, technology provider, or other third party as applicable.

E. Agreement Format and Timing

1. CFBHN may satisfy BAA documentation requirements through incorporated BAA provisions into a contract or a standalone BAA, as appropriate.
2. For NSPs and other provider relationships, BAA provisions are incorporated into the subcontract or purchase agreement.
3. For vendors and other third parties, a standalone BAA may be used.
4. The applicable agreement containing BAA provisions, or a standalone BAA, must be executed by individuals with appropriate signing authority for the parties.
5. Required BAA provisions must be in place before PHI/ePHI is created, received, maintained, transmitted, accessed, used, disclosed, exchanged, or otherwise made available under the relationship.
6. Required BAA provisions must also be in place before an NSP, vendor, contractor, consultant, technology provider, network partner, or other third party is permitted to receive system credentials, access applications, access data systems, enter areas where PHI/ePHI may be available, or perform services that may involve PHI/ePHI.

F. Review of External Business Associate Agreements

1. Vendor-provided BAAs must be reviewed before signature to confirm that the agreement accurately reflects the parties' roles and contains required HIPAA provisions.
2. Review may include Contracts, CFBHN HIPAA Privacy Officer, legal counsel, and/or other appropriate departments, depending on the nature of the relationship.
3. The review should evaluate whether the agreement adequately addresses, as applicable:
   a. Permitted uses and disclosures of PHI/ePHI;
   b. Privacy and security safeguards;
   c. Breach reporting and security incident reporting;

Business Associate Agreements (continued)

d. System access and access termination;
e. Subcontractor requirements;
f. Return, destruction, or continued protection of PHI/ePHI;
g. Indemnification, insurance, and limitation of liability provisions; and
h. Any conflicting obligations or terms inconsistent with CFBHN requirements.

G. Evaluation of Agreement Need
1. The need for BAA provisions is evaluated based on the nature of the services, data access, system access, facility access, provider subcontract, purchase agreement, purchase order, vendor agreement, technology agreement, data sharing arrangement, or other relationship that may involve PHI/ePHI.
2. When the need for BAA provisions is unclear, the matter is referred to legal counsel for review before PHI/ePHI or system access is granted.

H. Vendor-provided or provider-provided BAA are reviewed by Contracts, CFBHN's HIPAA Privacy Officer, and/or legal counsel as appropriate before signature to confirm that the agreement accurately reflects the parties' roles, contains required HIPAA provisions, does not create conflicting obligations, and adequately addresses breach reporting, system access, subcontractors, return or destruction of PHI/ePHI, indemnification, insurance, and other CFBHN requirements.

II. HIPAA Compliance

A. NSP compliance with applicable network participation, system access, data-use, privacy, security, training, reporting, and contractual requirements may be monitored by the CQI department during annual reviews or other monitoring activities, including under the COSO (Committee of Sponsoring Organizations of the Treadway Commission) framework.

B. NSPs 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 DCF HIPAA training required annually of NSPs with access to CFBHN data systems.
4. Conduct risk analysis, and adhere to contract, HIPAA, 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.
6. Notify CFBHN within 24 hours when a user no longer requires access to a CFBHN or DCF data system.

Business Associate Agreements (continued)

C. 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.

D. CFBHN 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.

E. CFBHN 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 CFBHN 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 CFBHN 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.

F. In the event of an impermissible use or disclosure of PHI, CFBHN 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.

G. 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.

H. 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. CFBHN's Information Technology department maintains responsibility for all user access to CFBHN's network data systems. Carisk Partners maintain responsibility for all user access to the Carisk Portal.

B. Before system access is granted to NSPs, vendors, contractors, consultants, technology providers, subcontractors, or other third parties, CFBHN will confirm that required agreements, BAA provisions, training, approvals, and access restrictions are in place.

C. NSP compliance with the terms of this policy are monitored by the CQI department during annual reviews of each organization. Reviews require the completion of a HIPAA Compliance affidavit by the NSP's HIPAA Privacy or Security Officer to verify that:

1. The NSP has appointed a formal Privacy and Security Officer.
2. HIPAA policies and procedures have been developed by the organization.

Business Associate Agreements (continued)

3. Staff training on HIPAA policies and procedures occurs at the time of hire and at regular intervals thereafter.
4. Such additional items as required by the CQI or Contracts.
5. When a user no longer requires access to a network data system, CFBHN is notified immediately, but no later than 24 hours to discontinue data system access.

Business Associate Agreements Approval: Alan Davidson, President/Chief Executive Officer	Date Issued: 04/01/2003 Last Revision: 08/19/2026 Review Date: 08/19/2026