HIPAA Sanctions

Policy
It is the policy of Central Florida Behavioral Health Network, Inc. (CFBHN) to ensure the confidentiality and integrity of the Protected Health Information (PHI) of employees and individuals served by the Network.

Purpose
This policy has been established to meet the requirements of the Health Insurance Portability and Accountability Act (HIPAA), 164.530 (e)(1). It outlines the application of sanctions to members of its workforce and Business Associates who fail to comply with privacy and security guidelines related to the handling of PHI.

I. Definitions

A. Business Associate: A person or organization that performs certain functions or activities that involve the use or disclosure of PHI on behalf of a covered entity, or to a covered entity. CFBHN maintains Business Associate Agreements (BAAs) with each of its subcontracted Network Service Providers (NSPs).

B. Protected Health Information (PHI): Data that is created, maintained, stored and transmitted in the provision of healthcare services that identifies, or could reasonably identify, the individual in care.

C. Whistleblower: An individual who, acting in good faith on the belief that CFBHN or one of its Business Associates has engaged in unlawful conduct, violates professional or clinical standards, or shares PHI with an unauthorized party.

D. Workforce: Employees, volunteers, trainees, or other persons whose conduct, in the performance of work, is under the direct control of CFBHN, whether or not they are paid by CFBHN.

II. Unauthorized Disclosures of PHI Made by Members of the CFBHN Workforce

A. As defined in the CFBHN *Confidentiality of Persons Served/Minimum Necessary Requirements* policy, members of the workforce are required to adhere to guidelines established by federal and state laws related to the confidentiality of persons served, and the protection of PHI.

1. Access to a DCF or CFBHN-hosted data system is granted to workforce members only after they have formally requested access by completing the *System Access Request Packet* and required data security training. This process is outlined in CFBHN's *Data System Access Management* policy.

2. At the time of hire, and on an annual basis, workforce members sign the *Privacy, Security and Risk Mitigation Guidelines for Staff Working Remotely* form that outlines the special precautions required of staff when working remotely, and handling PHI.

B. Members of the workforce who observe, or are aware of, a violation involving the protection of PHI are required to immediately report it to the Risk Manager, or as an incident through the RLDatix system. This process is documented in CFBHN's *Internal Incident and Event Reporting* policy.

HIPAA Sanctions (continued)

1. The Risk Manager:
   A) Reviews the content of the unprotected data to determine if it meets the definition of PHI.
   B) Conducts an assessment of the incident to determine the level of risk the violation presents to the subject, sender, recipient and CFBHN.
   C) Reaches out to the individual(s) involved to alert them of the violation.
   D) Documents each of these steps in the RLDatix incident record.

2. If the Risk Manager determines that the failure to protect PHI is a repeat violation by a member of the CFBHN workforce, or if the circumstances of the event may require sanctions, he or she will convene a review by the Sanctions Review Committee. The Sanctions Review Committee:
   A) Includes:
      1) The CFBHN Risk Manager,
      2) CFBHN's Privacy Officer,
      3) CFBHN's Security Officer,
      4) A representative of CFBHN's Human Resources department, and
      5) The workforce member's supervisor.

   B) Will meet to:
      1) Investigate and confirm the circumstances of the violation.
      2) Review the circumstances of the violation that may mitigate, or increase, the applied sanction.
      3) Consider the sanctions to apply to the workforce member.
      4) Make a sanctions recommendation to the Present/Chief Executive Officer (CEO) for review and approval.

3. If additional steps or notifications are warranted, the Risk Manager will consult CFBHN's Privacy, Security and/or Compliance Officer. This process is outlined in CFBHN's *Data Security Incident Response and Reporting Requirements* policy.

III. Unauthorized Disclosures of PHI Made by Business Associate Staff

A. Access to a DCF or CFBHN-hosted data system is granted to staff members of a Business Associate only after they have completed the *System Access Request Packet* and required data security training. This process is outlined in CFBHN's *Data System Access Management* policy.

B. Members of the CFBHN workforce who observe, or are aware of, a Business Associate staff member's failure to protect PHI must immediately report it to the Risk Manager, or as an incident through the RLDatix system. This process is documented in CFBHN's *Internal Incident and Event Reporting* policy.

   1. The Risk Manager:
      A) Reviews the content of the unprotected data to determine if it meets the definition of PHI.
      B) Conducts an assessment of the incident to determine the level of risk the violation presents to the subject, sender, recipient and CFBHN.
      C) Reaches out to the individual(s) involved to alert them of the violation.
      D) Documents each of these steps in the RLDatix incident record.

2. If the Risk Manager determines that the failure to protect data is a repeat violation by the Business Associate, or if the circumstances of the event may require sanctions, he or she will convene a review by the Sanctions Review Committee, as described in section II.B.2 of this policy.

3. If additional steps or notifications are warranted, the Risk Manager will consult CFBHN's Privacy, Security and/or Compliance Officer. CFBHN's *Data Security Incident Response and Reporting Requirements* policy outlines the components of its breach notifications process.

IV. Application of Sanctions

A. The Risk Manager and/or Sanctions Review Committee review the details of the violation and make a sanctions recommendation, in writing, to CFBHN's President/CEO.

B. In making a sanction recommendation, CFBHN will consider the details of the violation, including, but not limited to, the following:

1. Impact(s) of the PHI disclosure;

2. History of violations by the workforce member or Business Associate;

3. The nature, or type, of violation:

A) Accidental or Inadvertent Disclosures

1) Defined as: An unintentional violation of privacy or security that is caused by carelessness, lack of knowledge or human error.
2) Examples of this type of violation include, but are not limited to:
   a. Leaving PHI on a fax machine or copier.
   b. Emailing a clinical record to the wrong party.
   c. Mislabeling/misidentifying a health record.

B) Failure to Follow Established Privacy/Security Policies

1) Defined as: Performance that is contrary to established policy and procedure.
2) Examples of this type of violation include, but are not limited to:
   a. Discussing PHI in a public area.
   b. Walking away from a computer in a public area without securing PHI.
   c. Inadvertent release of PHI without appropriate documentation of the individual's authorization.
   d. Improper storage or disposal of PHI.
   e. Failure to report privacy or security violations.
   f. Transmission of PHI using an unsecured method.

C) Purposeful Violation

1) Defined as: An intentional violation designed to gather personal information about another individual without a legitimate reason to do so.
2) Examples of this type of violation include, but are not limited to:
   a. Accessing PHI on a family member or friend.
   b. Reviewing the client record of a high-profile individual or celebrity.

HIPAA Sanctions (continued)

D) Purposeful and Malicious Violation with Harmful Intent
1) Defined as: An intentional violation which involves accessing, reviewing, or disclosing PHI for personal gain, or to cause an individual, or the organization, harm.
2) Examples of this type of violation include, but are not limited to:
a. Accessing PHI with the intent to share it with others or the media.
b. Disclosing PHI to shame an individual or cause them harm.
c. Accessing or disclosing PHI for an illegal purpose, such as identity theft.

4. Mitigating circumstances of the violation that, if present, could support reducing the recommended sanction. Mitigating factors considered include, but are not limited to:

A) The individual who committed the violation acted in good faith in an attempt to help a client receiving services.
B) The violation resulted in no financial, reputational or personal harm to CFBHN, the Business Associate or the individuals impacted.
C) The individual acknowledged the violation, reported it in a timely manner and cooperated with the investigation.
D) Action taken was under pressure from an individual in a position of authority, or as the result of corporate culture that fostered inappropriate business practices.

5. Circumstances of the violation that, if present, may require an increase to the recommended sanction. Examples include, but are not limited to:

A) The violation involved a high volume of data or impacted individuals.
B) Significant expense to CFBHN or the Business Associate was incurred as a result of the violation.
C) The violation involved data that is subject to special protections. For example, records related to HIV or substance use.
D) The individual(s) involved:
1) Has a history of performance issues and/or previous violations.
2) Did not report it in a timely manner, was not truthful about their actions, or hampered an investigation into the incident.
3) Experienced personal gain as a result of the violation.

C. Sanctions considered in response to a violation, include, but are not limited to, the options listed below or a combination thereof:

1. Notice of violation to the workforce member or Business Associate staff member, their supervisor, Human Resources Manager and/or CEO.
2. Required repeat of HIPAA data security training.
3. Initiation of a staff performance improvement plan.
4. Documentation of the violation in the workforce member or Business Associate's personnel file.
5. Enhanced supervisor oversight when required to share PHI as a component of job duties.

HIPAA Sanctions (continued)

6. Suspension of the workforce member's, or Business Associate's, access to CFBHN/DCF data systems.
7. Notice to the Business Associate that requirements of the Business Associate Agreement have not been met.
8. Termination of workforce member, or Business Associate staff, access to CFBHN/DCF data systems.
9. Termination of workforce member employment.
10. Termination of a Business Associate Agreement.

D. The final decision on the application of sanctions rests with the CFBHN President/CEO.

IV. Sanction Exemptions and Policy of No Retaliation

A. Sanction exemptions and the policy of no retaliation described in this section is applicable to members of the CFBHN workforce, and staff members of CFBHN Business Associates.

B. A disclosure made by an individual identified as a whistleblower is not subject to the sanctions defined in this policy. Examples of whistleblower disclosures that are exempt from sanctions include, but are not limited to, reports made to:
   1. The Department of Children and Families;
   2. Federal or state health oversight agencies or public health organizations;
   3. Accreditation organizations;
   4. An attorney retained on behalf of the whistleblower for the purpose of determining legal options regarding disclosure conduct.

C. A disclosure made by an individual who is the victim of a crime is not subject to the sanctions defined in this policy if:
   1. The victim of the criminal act discloses PHI to a law enforcement official about the suspected perpetrator; and
   2. The disclosed information is limited to that which is necessary to identify or locate the individual.

D. CFBHN policy does not permit intimidation, threats, coercion, discrimination or other retaliatory behaviors against an individual who:
   1. Exercises their right to file a data security-related complaint to a federal or state authority.
   2. Testifies, assists or participates in a data security-related investigation, compliance review, proceeding or hearing.
   3. Is recognized as a whistleblower, or victim of a crime, as defined in the previous section of this policy.

HIPAA Sanctions Approval: Alan Davidson, President/Chief Executive Officer	Date Issued: 03/03/2022 Last Revision: 04/28/2023 Review Date: 07/31/2024