Health Insurance Portability and Accountability Act 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
The purpose of this HIPAA Sanctions Policy is to ensure compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), including the HIPAA Privacy Rule, Security Rule, and Breach Notification Rule. This policy establishes a framework for applying appropriate sanctions against workforce members who fail to comply with HIPAA requirements, organizational policies, or procedures related to the protection of PHI

I. Definitions

A. 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.

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

C. Violation: Any act or omission that fails to comply with HIPAA or organizational policies related to privacy or security.

II. Scope

A. This policy applies to:
   1. All members of the workforce of CFBHN, including but not limited to: employees, volunteers, contractors, temporary staff and/or other individuals whose conduct is under the direct control of the organization.
   2. Violations involving PHI in any form, including electronic (ePHI), paper, and oral communications.

B. Workforce members receive training on HIPAA requirements and this Sanctions policy upon hire and periodically thereafter. Workforce members are responsible for understanding and complying with this policy.

C. CFBHN takes appropriate disciplinary action against workforce members who violate HIPAA regulations, organizational privacy and security policies, or applicable procedures.
   1. Sanctions will be applied in a manner that is:
      a. Consistent,
      b. Proportionate to the severity of the violation,
      c. Documented, and
      d. In accordance with applicable laws and human resources policies.

   2. No retaliation is taken against individuals who report suspected HIPAA violations in good faith.

D. The policy is reviewed annually and updated to reflect changes in laws regulations or organizational practices.

Health Insurance Portability and Accountability Act Sanctions
(continued)

III. Types of HIPAA Violations

A. HIPAA violations may include, but are not limited to:
1. Unauthorized access to PHI. Example: Unauthorized viewing patient records
2. Unauthorized use or disclosure of PHI
3. Failure to safeguard PHI . Example: Leaving records open and unattended
4. Sharing passwords or login credentials
5. Failure to follow security procedures
6. Improper disposal of PHI
7. Failure to report a suspected breach or incident
8. Retaliation against individuals who report compliance concerns

B. Reporting Violations

1. Workforce members must promptly report suspected or known HIPAA violations to:
   a. A supervisor
   b. The Privacy Officer
   c. The Compliance Hotline or other designated reporting mechanism
2. Reports may be made without fear of retaliation.

IV. Application of Sanctions

A. Sanctions will be determined based on factors such as intent, severity, harm, history of prior violations, and whether the violation was accidental or malicious.
1. Level 1 – Minor or Unintentional Violations
   a. Examples
      1) Inadvertent access without further use or disclosure
      2) First time failure to follow procedure
   b. Possible sanctions
      1) Verbal counseling
      2) Re-training or re-education
      3) Written warning

2. Level 2 – Moderate Violations
   a. Examples
      1) Repeated minor violations
      2) Careless handling of PHI
      3) Failure to report a known incident
   b. Possible sanctions
      1) Written reprimand
      2) Mandatory re-training
      3) Suspension of system access

3. Level 3 – Serious Violations
   a. Examples
      1) Intentional or malicious access, use or disclosure of PHI
      2) Disclosure for personal gain
      3) Significant harm to patients or the organization
   b. Possible sanctions
      1) Termination of employment or contract
      2) Reporting to licensing boards or professional authorities

3) Civil or criminal referral when required by law

V. Investigation and Enforcement

A. All suspected HIPAA violations are promptly investigated by the Privacy Officer, Security Officer, Human Resources, or other designated personnel. Investigations are conducted confidentially to the extent possible.

B. The organization reserves the right to determine the appropriate sanction based on the findings of the investigation.

C. Violations that are determined to involve potential violations of federal law, state statutes, or professional licensing standards will be escalated to the appropriate authority as required by the applicable regulation. This may include, but is not limited to, notifications to law enforcement, state or federal oversight agencies, or professional licensing boards.

D. All sanctions imposed under this policy will be documented and retained in accordance with organizational record retention policies and HIPAA documentation requirements.

HIPAA Sanctions Approval: Alan Davidson, President/Chief Executive Officer	Date Issued: 03/03/2022 Last Revision: 08/20/2026 Review Date: 08/20/2026