PHOENIX
COUNSELING CENTER
Where Help, Hope and Compassion Come Together

PHOENIX COUNSELING CENTER
POLICY AND PROCEDURE

Title: Health Insurance Portability and Accountability Act (HIPAA) Contingency Plan	**Policy Number:** I-D-005-11 **Effective Date:** 11/18/2020
Responsible Department: IT	**Board Chair:** Heidi Chui **Date:** 11/18/20
Last Revision:	**CEO:** [signature] **Date:** 11/18/2020
Board Reviews:	

POLICY:

A. It shall be the policy of Phoenix Counseling Center (PCC) to comply with Health Insurance Portability and Accountability Act (HIPAA) regulations regarding Contingency Plan, which includes contingency plan, data backup plan, disaster recovery plan, emergency mode operation plan, testing and revision procedures, applications and data criticality analysis, and contingency operations.
B. The purpose of this policy is to establish rules to protect the availability, integrity and security of electronic protected health information (EPHI) from the impact of natural, human, and environmental risks while continuing business without the normal resources of the organization.

PROCEDURE:

A. PCC shall have documented procedures for implementation in the event of an emergency, disaster or other occurrence (i.e., fire, vandalism, system failure, and natural disaster) when any system that contains EPHI is affected, including:
   1. Applications and Data Criticality Analysis
   2. Data Backup Plan
   3. Disaster Recovery Plan
   4. Emergency Mode Operation Plan

B. Each of the following plans shall be evaluated and periodically updated as business needs and technology requirements change.
   1. Applications and Data Criticality Analysis
      a. PCC shall periodically assess the relative criticality of applications and data used by the HIPAA covered component for purposes of maintaining a current Data Backup Plan, Disaster Recovery Plan and Emergency Mode Operation Plan.
      b. PCC shall identify critical business functions, define impact scenarios, and determine resources needed to recover from each impact.
   2. Data Backup Plan
      a. All EPHI shall be stored or backed up individually or to network servers.
      b. Information Technology (IT) shall establish and implement a Data Backup Plan that, at a minimum, includes daily backups of user-level and system-level information and weekly backups that are stored securely offsite.
      c. The Data Backup Plan shall apply to all files that may contain EPHI.

d. The Data Backup Plan shall require that all media used for backing up EPHI be stored in a physically secure environment.
e. Data backup procedures outlined in the Data Backup Plan shall be tested on at least an annual basis to ensure that exact copies of EPHI can be retrieved and made available.

3. Disaster Recovery Plan
   a. To ensure that PCC can recover from the loss of data due to an emergency or disaster such as fire, vandalism, system failure, or natural disaster affecting systems containing EPHI, IT/support shall establish and implement a Disaster Recovery Plan for restoring or recovering loss of EPHI and the systems needed to make that EPHI available in a timely manner.
   b. The Disaster Recovery Plan shall be documented and be available to the assigned personnel who shall be trained to implement the Disaster Recovery Plan.
   c. The disaster recovery procedures outlined in the Disaster Recovery Plan shall be tested on a periodic basis to ensure that EPHI and the systems needed to make EPHI available can be restored or recovered.
4. Emergency Mode Operation Plan
   a. PCC shall document and implement procedures to enable continuation of critical business processes for the protection of EPHI while operating in emergency mode. Emergency mode operation must include processes to protect the security of EPHI during and immediately after a crisis.
   b. Emergency mode operation procedures outlined in the Disaster Plan for each location/site.

C. Policy Responsibilities
1. Manager and Supervisor
   a. Annually ensure that appropriate emergency operations and disaster recovery procedures are in place.
   b. Periodically test their Emergency Operations Mode Plan.
   c. Ensure that workforce members save all EPHI on network drives and not on the local drive (C:) of their workstation.
2. IT Director Support
   a. Develop and document an Emergency Operations Mode Plan for their units that include appropriate procedures for their workforce.
   b. Establish, implement and document the Data Backup Plan for EPHI used at PCC.
   c. Annually test the EPHI backups to ensure that exact copies of EPHI can be retrieved.
   d. Document and maintain a Disaster Recovery Plan to restore the EPHI applications and data that is needed for the HIPAA covered components to continue their critical business functions in a disaster.
   e. Periodically test the documented disaster recovery procedures to ensure EPHI data and systems can be restored.