Policy Number: HC-24	Page: 1	Of: 3
Title: Disaster Recovery Plan and Emergency Mode Operation		
Regulatory Authority: HIPAA Regulations, FERPA Regulations, ORC, OAC		
Effective Date: 01/19/2021		
Reviewer/Job Title: Director of Operations		

(A)DISASTER RECOVERY PLAN AND EMERGENCY MODE OPERATION
Board personnel shall develop contingency plans to prepare for system failures, and for procedures for maintaining critical board operations in the event of system failure.

Audience

Hipaa privacy/security officer

Authority

HIPAA Privacy and Security Rules, 45 CFR Part 164

164.308(a)(7)

164.312(a)(1)

References

NIST SP 800-14

NIST SP 800-18

NIST SP 800-26

NIST SP 800-30

NIST SP 800-53

1) **Disaster Recovery Team**. If appropriate, the HIPAA Security Officer shall establish a Disaster Recovery Team to assist in the preparation of contingency plans as well as to execute assigned tasks in the event of a disaster. The HIPAA Security Officer shall direct this team and is responsible for all tasks identified in this policy.
2) **Scenario Identification**. Contingency planning shall begin with identification of likely failure scenarios. These scenarios should include, at a minimum, failure of one or more servers, data corruption of one or more subsystems, and catastrophic loss of the entire

facility due to fire or other natural disaster. These scenarios shall be included in the written plan, and serve as the basis for the measures outlined below.

3) **Preventative Measures**. The HIPAA Security Officer shall, on an ongoing basis, evaluate the activities that are critical to board operations and implement preventative measures to reduce the likelihood of system failure. These would include technical measures such as backup power supplies, fire suppression systems, raised floors, security systems, database transaction logging and the like.
4) **System and Data Recovery Plan**. The HIPAA Security Officer shall maintain a written system and data recovery plan, and take reasonable steps to mitigate losses, for likely failure scenarios. The written plan should include:
   a) Computer applications shall be reviewed and assessed as to their criticality for maintaining board operations. The results of this assessment shall be documented.
   b) Development of written documentation of tasks and responsibilities for members of the Disaster Recovery Team in the event of various failure scenarios.
   c) System configuration documentation, as specified in the policy "HIPAA Security Officer and Security Management Process" to facilitate replacement of vital equipment in the event of a catastrophic loss.
   d) Complete and current employee information and vital records.
   e) Identification of, and contact information for, vendors who will be used for replacing equipment following a disaster.

Reasonable steps to assure rapid recovery and mitigate losses can include, if appropriate:

   a) Contracts with any necessary consultants and/or vendors to facilitate recovery, if deemed necessary and prudent by board management.
   b) Contracts with hot and/or cold system sites if deemed necessary and prudent by board management.
   c) Steps to manage risk, such as insurance policies, as deemed appropriate, for possible losses to mitigate the financial impact of disasters.

5) **Emergency Mode Operations Plan**. The HIPAA Security Officer shall maintain a plan to maintain vital operations in the event of a partial or complete system failure. This should begin with an identification of likely failure scenarios as described above. Elements of this plan may include:
   a) Identification of situations which occur where immediate access to Individual data is necessary, as in certain MUIs involving health emergencies,
   b) Maintenance of Critical Individual Data from electronic in a paper chart, or other plan to protect against loss of access due to technical failure,
   c) People assigned to assist Case Managers or other individuals with immediate access to this information in the event of an emergency regarding an Individual (accident, medical incident, etc.)
   d) Periodic training of staff, regarding how to access information in the event of simultaneous computer downtime and Individual emergency,
   e) For non-emergency situations, procedures which allow staff to function, to the extent possible, in the event of system downtime.

6) **Plan Testing**. The HIPAA Security Officer shall be responsible for plan testing. He or she shall design the approach to testing and the level of resources which are appropriate to invest in these activities based on the risk analysis.
7) **Off Site Storage of Key Documents**. A copy of the key documents described in this policy shall be maintained off site, in either paper or electronic form, so that they are readily and quickly assessable in the event of catastrophic loss of the facility.