BUSINESS CONTINUITY PLANNING & INFORMATION TECHNOLOGY DISASTER RECOVERY

Policy: The purpose of this policy is to address the minimum features that must be documented and implementable in plans that are developed for emergency situations.

Rationale: To comply with 45 CFR 164.308 to ensure that plans are developed to respond to emergency or similar occurrences.

POLICY STATEMENT:

The HIPAA Security rule requires that HIPAA Covered Entities create, implement and test contingency plans to respond to allow for business continuity and disaster recovery of data and systems in emergency or similar situations.

Each HIPAA Covered Component shall create and implement a contingency plan to deal with emergency situations. A contingency plan is the most appropriate approach to protect availability, integrity and security of data during negative events that may occur outside of the organization's control. Five standard contingency planning components are identified within the HIPAA Security Rule:

1. **Data Backup Plan** – 45 CFR 164.308 (a) (7) (ii) (A) requires Covered Entities to establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.
2. **Disaster Recovery Plan** – 45 CFR164.308 (a) (7) (ii) (B) requires Covered Entities to establish (and implement as needed) procedures to restore any loss of data.
3. **Emergency Mode Operation Plan** – 45 CFR 164.308(a) (7) (ii) (C) requires Covered Entities to establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information (ePHI) while operating in emergency mode.
4. **Testing and Revision Procedures** – 45 CFR 164.308(a) (7) (ii) (D) requires Covered Entities to implement procedures for periodic testing and revision of contingency plans.
5. **Applications and Data Criticality Analysis**– 45 CFR 164.308 (a) (7) (ii) (E) requires Covered Entities to assess the relative criticality of specific applications and data in support of other contingency plan components.

Implementation

A Contingency Plan is a written set of instructions focused on how to sustain mission/business processes during and after a disruption.

Each HIPAA-Covered Component shall develop a Contingency Plan for responding to an emergency or other occurrence (for example, fire, vandalism, system failure and natural disaster) that damages IT resources that contain ePHI.

The Contingency Plan shall include the following components:

1. An application and data criticality analysis shall be developed, documented and maintained to assess the relative criticality of specific applications and data in support of the contingency plan components.

2. Facility access procedures shall be developed, documented and maintained for access to support recovery efforts.

3. Contingency plan testing and revision procedures shall be developed, documented and periodically executed for verifying recovery capabilities.

4. A data backup plan shall be established, documented and implemented to create and maintain retrievable exact copies of ePHI.

5. Emergency access procedures shall be established, documented and implemented for the retrieval of ePHI during an emergency.

6. A disaster recovery plan shall be established, documented, implemented and tested to restore any loss of data in the event of a disaster.

7. An emergency mode operations plan shall be developed, documented and implemented to protect ePHI during emergency operations of business processes.

Reference: 45 CFR 164.308