**AS—07 Contingency Plan**

***Purpose***

To establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information. 164.308(a)(7)(i)

**Guidance**

* Back up original sources of essential ePHI on an established schedule.
* Backup copies must be securely stored in a physically separate location from the data source.
* Backups containing ePHI will be transported via secure methods.
* Documentation must exist to verify the creation of backups and their secure storage.

**Data backup plan**

Implementation: To establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information. 164.308(a)(7)(ii)(A)

**Disaster recovery plan**

Implementation: To establish (and implement as needed) procedures to restore any loss of data. 164.308(a)(7)(ii)(B)

* To establish procedures to restore loss of essential ePHI that resulted from a disaster or emergency.
* Copies of the data restoration procedures must be readily accessible at more than one location and should not rely on the availability of local power or network.
* Backup procedures must include steps to ensure that all protections (patches, configurations, permissions, firewalls, etc.) are re-applied and restored before ePHI is restored to a system.

**Emergency mode operation plan**

Implementation: To establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode. 164.308(a)(7)(ii)(C)

* To ensure that HIPAA entity emergency operations procedures maintain security protections for ePHI.
* To evaluate operations in emergency mode, e.g. a technical failure or power outage, to determine whether security processes to protect ePHI are maintained.
* To document assessment and conclusions.
* To document and implement additional authorities and procedures necessary to ensure the continuation of security protections for ePHI during emergency operations mode.

For evacuations:

* HIPAA entities' emergency response plans shall include logging out of systems that contain ePHI, securing files, and locking up before evacuating a building, if safe to do so.
* HIPAA entities should have processes to ensure there was no breach when the area is re-occupied.

**Testing and revision procedures**

Implementation: To develop procedures for periodic testing and revision of contingency plans. 164.308(a)(7)(ii)(D)

* Document the contingency plan procedures.
* Ensure that those responsible for executing contingency plan procedures understand their responsibilities.
* Periodically, and at least annually, perform a test of the contingency plan procedures.
* Document test results, review and correct any problems with the test, and update procedures accordingly.

**Applications and data criticality analysis**

Implementation: To assess the relative criticality of specific applications and data in support of other contingency plan components. 164.308(a)(7)(ii)(E)

To prioritize criticality of applications and data sets for data backup, restoration, and application of emergency mode operation plan.

Priorities can be included in data restoration procedures (§164.308(a)(7)(ii)(B) - Disaster recovery plan).