

Data Backup and Recovery

- ❖ § 164.308 Administrative safeguards.
- ❖ (7)(i) *Standard: Contingency plan*. 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.
- ❖ (ii) *Implementation specifications*:
- ❖ (A) *Data backup plan (Required)*. Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.
- ❖ (B) *Disaster recovery plan (Required)*. Establish (and implement as needed) procedures to restore any loss of data.
- ❖ (C) *Emergency mode operation plan (Required)*. 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.
- ❖ (D) *Testing and revision procedures (Addressable)*. Implement procedures for periodic testing and revision of contingency plans.
- ❖ (E) *Applications and data criticality analysis (Addressable)*. Assess the relative criticality of specific applications and data in support of other contingency plan components.