Policy Number:		**Effective Date: __/__/____**
Subject:	**Policies for Administrative Safeguards**	**Revised: __/__/____**
Policy Name:	**Disaster Recovery Plan (Required)**	**Approved:_____**

POLICY

[Organization] will establish a written plan to restore data lost through occurrence of a disaster and to maintain the confidentiality of electronic data during the duration of the disaster.

GUIDELINES FOR DEVELOPING A DISASTER RECOVERY PLAN

1. [Organization's] risk analysis will identify the potential hazards that could result in loss of electronic data, including natural threats (earthquake, flood, etc.), environmental threats (power failure, etc.) and human threats.

2. [Organization's] written disaster recovery plan shall specify the triggering events that will activate the plan.

3. [Organization's] disaster recovery plan shall encompass the following objectives:
    - Providing for the safety and well-being of workforce members and other individuals
    - Continuing critical business operations and data functions
    - Minimizing the duration of a serious disruption to operations and resources
    - Minimizing immediate damage and losses
    - Establishing management succession and emergency powers
    - Facilitating effective co-ordination of recovery tasks
    - Reducing the complexity of the recovery effort
    - Identifying critical lines of business and supporting functions

4. [Organization's] disaster recovery plan shall prioritize critical data functions that are most essential to maintaining patient care at [Organization].

5. The disaster recovery plan shall include identification of and contact information for resources needed to support critical functions, including but not limited to:
    - Personnel
    - Processing capabilities
    - Alternative space
    - Computer-based services (such as telecommunications)
    - Other alternative equipment
    - Data and applications
    - Physical infrastructure

6. The disaster recovery plan shall establish teams of individuals who will be responsible for securing the critical resources noted above. The plan shall identify each team member and his or her specific tasks and responsibilities.

7. The disaster recovery plan shall include procedures for accurately assessing damage to electronic data incurred as a result of the disaster.

8. The disaster recovery plan shall include strategies to achieve prompt recovery of critical functions and electronic data, in the event of an occurrence of each of the hazards identified in the risk analysis.

9. The disaster recovery plan shall include strategies to maintain the confidentiality of electronic data during the recovery process.

10. [Organization] shall determine system vulnerability to significant service interruptions and define within the plan preventative measures that may be taken to minimize the probability and impact of interruptions.

11. The disaster recovery plan shall address immediate, intermediate and long-term recovery needs and resource requirements.

12. The disaster recovery plan shall be reviewed and, if necessary, updated at least every [six months, year, etc.].

**Please note: Most organizations already have an organization-wide disaster recovery plan in place. The purpose of this policy is to give organizations guidelines for developing a disaster recovery plan specifically incorporating the requirements of the Security Regulations, namely to ensure that the security of electronic data is taken into account when a disaster recovery plan is created. Organizations may prefer to incorporate additional safeguards concerning electronic data into their existing disaster recovery plans.*

REFERENCES

See also
Security Risk Analysis Policy
Security Risk Management Policy
Data Backup Plan Policy
Emergency Mode Operations and Emergency Access Procedures Policy
Applications and Data Criticality Analysis

45 C.F.R. § 164.308(a)(7)(ii)(B)

