Education Blast
APRIL 2017

Contingency Plan

§164.308(a)(7)(i) states that organizations are required 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.

Key activities.

- **Develop contingency planning policy**
- **Conduct an applications and data criticality analysis**
- **Identify preventive measures**
- **Develop recovery strategy**
- **Data backup plan and disaster recovery plan**
- **Develop and implement an emergency mode operation plan**
- **testing and revision procedure**

It also states the specific activities listed below should take place periodically.

- Implement:
  - **Data Backup Plan (Required)**. Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information
  - **Disaster Recovery Plan (Required)**. Establish (and implement as needed) procedures to restore any loss of data
  - **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
  - **Testing and Revision Procedure (Addressable)**. Implement procedures for periodic testing and revision of contingency plans

- **Applications and Data Criticality Analysis (Addressable)**. Assess the relative criticality of specific applications and data in support of other contingency plan components

As you implement your policies and procedures here are some questions to ask yourself.

- What critical services must be provided within specified timeframes?
- Have cross-functional dependencies been identified so as to determine how the failure in one system may negatively impact another one?
- What hardware, software, and personnel are critical to daily operations?
- What is the impact on desired service levels if these critical assets are not available?
- What is the nature and degree of impact on the operation if any of the critical resources are not available?
- What is the cost associated with the preventive measures that may be considered?
- Are the preventive measures feasible (affordable and practical for the environment)?
- What plans, procedures or agreements need to be initiated to enable implementation of the preventive measures, if they are necessary?
- Have procedures related to recovery from emergency or disastrous events been documented?
- Is there a formal contingency plan?
- Have procedures been developed to continue the critical functions identified in Key Activity?
- How is the plan to be tested?
- Does testing lend itself to a phased approach?
- Can testing be done during normal business hours or must it take place during off hours?

Your Trusted Advisor,

healthPOINT at Dakota State University | SECURITY services

Questions?
Contact us: Email - HPSS@dsu.edu | Phone - (605) 256-5555