Oklahoma State University

Title: Applications and Data Criticality Analysis	**Policy #: SEC-06.05**
Category: HIPAA Compliance	**Authority: 45 CFR §** **HIPAA SECTION: 164.308(7)(ii)(E)**
Standard: Contingency Plan	**Responsibility: Health Care Components**
Effective Date: 4/20/2005	**Pages: Page 1 of 1**
Approved By: OSU Legal Counsel	**Revised: 7/1/2013**

PURPOSE:

To enable the continuation of critical business processes for protection of the security of EPHI during emergency mode operations.

POLICY:

Assess the relative criticality of specific applications and data in support of other contingency plan components.

PROCEDURE:

1. Activities and Materials that are critical to daily business operations include:
    a. Network services (i.e. firewalls, switches, fiber optic lines, wireless)
    b. Servers (i.e. authentication server, EMR server, PM server)
    c. Software (EMR, PM)
    d. Equipment (computers, printers)
2. Automated processes that support critical services or operations
        1. Network services (i.e. firewalls, switches, T1 lines, wireless)
        2. Servers (i.e. authentication server, EMR server, PM server)
        3. Software (EMR, PM)
        4. Equipment (computers, printers)
        5. IT personnel
3. Power outages disrupting network services, servers, and EMR application can only be tolerated for 24 hours. Practice Management disruption can only be tolerated for 72 hours.
4. In response to an emergency where servers were destroyed, a new server would be purchased and put in the most secure and reliable location. Data would be restored as described in the Data Backup Plan policy. Please see Contingency Plan policy for further details.

REFERENCE:

Data Backup Plan
Contingency Plan