**Applications and Data Criticality Analysis**

**Purpose:**

To enable the continuation of critical business processes, to protect and secure ePHI during emergency mode operations.

**Policy:**

Assess the relative criticality of specific applications and data in support of other contingency plan components. The criticality analysis will serve as the basis for the recovery prioritization of ePHI and ePHI Systems during the disaster recovery plan.

**Procedure:**

1. The Privacy Officer will meet with the Information Security Officer to identify any and all computers, systems, applications, and data which are critical to the organization’s operation.
2. The results will be documented on the Criticality Analysis tab of the Periodic Ledger workbook.
3. Data and AWS services will be restored as described in the Data Backup and Contingency Plan policies.
4. This procedure will be carried out annually or in response to changes with critical applications and data tracked on the Criticality Analysis Worksheet of the Periodic Task Ledger.