JORDAN VALLEY EMS AUTHORITY POLICY

POLICY #:	103.4.13	**SUBJECT:**	DISASTER MANAGEMENT AND RECOVERY OF PHI
CAAS STANDARD:	103.4	**SCOPE:**	ALL

PURPOSE:
The Authority is responsible for ensuring that we have a process in place to ensure that we can recover from the catastrophic disruption of our information system and loss of any data or information, especially e-PHI, which may be stored on that system. .

POLICY:
This policy will be followed in an emergency situation or disaster such as fire, vandalism, terrorism, system failure, or natural disaster. This policy applies to all the Authority staff members who create, receive or use PHI and e-PHI, and any other confidential patient or business information. It is intended to cover all information system hardware, software and operational procedures

PROCEDURE:
To ensure that the Authority will be able to recover from a serious information system disruption, including situations that could lead to the loss of data in the event of an emergency or disaster (such as fire, vandalism, terrorism, system failure, or natural disaster) the following procedures are established:

1. A disaster recovery plan will be established and implemented to restore or recover any loss of e-PHI and any loss or disruption to the systems required to make e-PHI available.
2. The disaster recovery plan will be developed by staff members responsible for the maintenance of the security and integrity of the information system and will be reviewed and approved by the Privacy/Information Security Officer and senior management.
3. The recovery plan will be maintained and reviewed by the IT Department Manager in consultation with the Privacy Officer
4. The disaster recovery plan must include:
    a. A data backup plan including the storage location of backup media.
    b. Procedures to restore e-PHI from data backups in the case of an emergency or disaster that results in a loss of critical data.
    c. Procedures to ensure the continuation of business critical functions and processes for the protection of e-PHI during emergency or disaster situations.
    d. Procedures to periodically test data backup and disaster recovery plans.
    e. Procedures to log system outages, failures, and data loss to critical systems.
    f. Procedures to train the appropriate personnel to implement the disaster recovery plan.
5. The disaster recovery plan must be documented and easily available to the necessary personnel at all times.

CURRENT PHI DISASTER RECOVERY PLAN:
The Authority will maintain physical back up of all essential data on premise in fire-rated safe with access limited to the EMS Director, Business Manager, and IT Manager.

In the event of a large scale disaster resulting a large scale failure of infrastructure, the IT Manager will work with service vendors to re-establish connections to infrastructure such as internet and telephone communications.

The IT Manager will be responsible for any periodic review and training of the disaster recovery plan.

POLICY HISOTRY:
Implemented February 1, 2015