JORDAN VALLEY EMS AUTHORITY POLICY

POLICY #:	103.4.16	**SUBJECT:**	FACILITY AND COMPUTER ACCESS CONTROLS
CAAS STANDARD:	103.4	**SCOPE:**	ALL

PURPOSE:

The company is responsible for ensuring the security of all patient information that we create, receive, or use under both the Privacy Regulations (Privacy Rule) and the Security Regulations (Security Rule) of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Due to its critical importance to the company, it is our obligation to control access to our physical locations where our electronic information system hardware, software, or other peripheral devices are stored or maintained. This policy describes our general approach to facility access under the Security Rule.

POLICY:

It is our policy to limit access to our electronic information system while at the same time, permit authorized access in the event of an emergency, or other events that require contingency plans to be placed in operation. The company will use the procedure detailed below to control access to facilities, vehicles and devices that contain PHI.

PROCEDURE:

Contingency Operations

1. The Information Security Officer will work with managers of the electronic information system to determine contingency plans and procedures that should be implemented in the event of the need to restore lost data and to maintain uninterrupted access to e-PHI.
2. Working with management of the company, the Information Security Officer will develop a list of persons who have permission to access computer systems and secured areas in the event that restoration and preservation of data is necessary.
3. The Information Security Officer, as part of the contingency plan, will develop and maintain a list of persons authorized to have access to the facility when the contingency plan is in operation.
4. The Information Security Officer will work with management to develop a “call list” of persons who need immediate notification when the contingency plan is in operation.
5. The Information Security Officer will work with the communications center and other points of access to the facility to determine their role and procedures to follow in the event the contingency plan is in operation.

Facility Security

1. The Information Security Officer will work with management to determine who should have access to e-PHI and the electronic information system and determine the extent of that access.
2. Care will be taken to ensure that limitation of access does not hinder our ability to provide essential information needed for treatment and transport of patients, billing for our services, and health care operations.
3. An inventory of all software and hardware will be developed and maintained by the IT Manager or Privacy/Information Security Officer to include:
    a. Assignment of identification numbers to hardware and other devices that are part of the electronic information system
    b. A record book or file will be maintained to catalog all software and hardware, with their unique identification numbers. The inventory will be conducted on at least an annual basis.
4. Any discrepancies in the current inventory of software and hardware in comparison to the last inventory will be reported to management and will be investigated to ensure that there is a proper accounting of all Universal software and hardware.
5. A central storage area for all original/licensed copies of software, source codes, etc. shall be created that is secure and environmentally safe so that the software is protected from destruction or damage as best as possible.

6. All company staff members who are approved for access to e-PHI sources and the electronic information system shall be assigned unique passwords where appropriate to ensure secure access to the system.
7. The Information Security Officer will work with management to develop keypad access systems so that access codes may be changed when staff members leave the organization or the list of approved persons for access to the electronic information system has been changed.
8. There will be a list of all keys and passport devices issued to personal who have access to the electronic information system to ensure accountability. The list will be developed and maintained by the Information Security Officer and updated as needed.

Access Control and Validation

1. Lists of persons with approved access to e-PHI and the electronic information system will be maintained to include lists of approved vendors and other outside parties who have permission to access our facilities and secure areas.
2. Software testing and other maintenance or service of the electronic information system will be carefully monitored by the Information Security Officer.
3. All guests and others with temporary access to the electronic information system that contains e-PHI shall sign appropriate confidentiality agreements. Access will be granted only upon presentation of verification of identity (such as a driver's license) and authorization to have access to the facility or access point.
4. The staff member permitting access to anyone other than an authorized staff member will document their name so as to be able to track who gave the person access.

Maintenance Records

1. The IT Manager will ensure that all repairs and maintenance to the electronic information system hardware or software is properly logged and documented.
2. The repair or maintenance records will contain, at a minimum:
    a. Name of person completing the maintenance or repair
    b. Purpose of the maintenance or repair
    c. Name of person authorizing it
    d. Date and time the work started and ended
    e. Brief description of the work completed and the outcome of it (more work required, alternative procedure to put in place, etc.)

Accountability

1. The IT Manager or Information Security Officer will develop a procedure to maintain and record the actions of any staff member or other person who adds hardware or software to our electronic information system.
2. Any hardware or software removed from the electronic information system will be signed in and signed out, with the signature of the person removing the hardware or software, and a corresponding signature of the Information Security Officer or other approved manager to acknowledge approval for the removal and responsibility for it.
3. No hardware or software will be added to the electronic information system without consultation with the Information Security,

POLICY HISTORY:
Implemented February 1, 2015