JORDAN VALLEY EMS AUTHORITY POLICY

POLICY #: 103.4.14 **SUBJECT:** SECURITY OF PHI

CAAS STANDARD: 103.4 **SCOPE:** ALL

PURPOSE:
The Authority is obligated to establish physical safeguards to protect Electronic Protected Health Information (e-PHI) and other PHI, confidential information and business information. This policy establishes our procedure with respect to security measures to protect our electronic information systems and related buildings and equipment from natural and environmental hazards, and unauthorized intrusion.

POLICY:
All of us must be on the lookout for any potential problems that could jeopardize the security of electronically stored information, especially e-PHI. This policy describes our general approach to facility security and the steps necessary to prevent a breach in the physical security system in place. It also describes our general procedures to limit physical access to electronic information systems and the buildings and rooms in which they are housed, and our general procedures on disposal or reissuance of computer equipment**.**

PROCEDURE:

Facility Access Controls
Access to areas of our facility that contain our information system components will be granted only to those with a verifiable and approved business need to have access.

Access control will be established with physical hardware that prevents improper or inadvertent entry into a secure area. This hardware may include combination locks, swipe cards, smart cards and other devices on all doors housing our information system equipment.

The Authority will retain facility security of any areas that we use within a building owned or under the control of another entity. In other words, any space in a building that we share with another entity will be maintained at the same level of security as if we owned the space. Specifically, we will protect that area from access by others in the building who are not part of the Authority.

Disabling or circumventing any of the physical security protections is strictly prohibited. Any problems with physical security measures must be reported to your supervisor or the Information Security Officer.

Contingency Operations. The Authority has established procedures that allow facility access in support of restoring lost data under our disaster recovery plan and emergency mode operations plan in the event of an emergency that could compromise our electronic information system.

Facility Security Plan. The Information Security Officer will be responsible for developing a facility security plan that protects our buildings from unauthorized physical access, tampering, and theft.

The plan will incorporate hardware to limit access to our buildings to only those persons with proper keys and/or access codes.

The Information Security Officer will maintain a current list of all staff members who have authorization to access our facilities. Where appropriate, the Authority will install security systems including video surveillance to protect our staff and to ensure the security of our information systems containing patient and other essential information.

Access to locations that house our information system infrastructure will have the greatest limitations on access, and access to these critical areas will be reviewed frequently by management and the Privacy/Information Security Officer.

JORDAN VALLEY EMS AUTHORITY POLICY

POLICY #: 103.4.14 **SUBJECT:** SECURITY OF PHI

CAAS STANDARD: 103.4 **SCOPE:** ALL

Workstation Security and Use

A "workstation" is defined as any electronic computing device, such as a desktop computer, laptop computer, PDA, or any other device that performs similar functions, and electronic media stored in its immediate environment.

All workstations will be evaluated to consider the procedures that must be followed to ensure the security of patient and other critical information. The environment will be considered (such as if the workstation is in a large room with cubicles and no fixed walls, the back of an ambulance, a crew room or report writing room, etc.)

General principles of our workstation security program include the following:

- All workstations (including both fixed locations such as in our billing or business office, as well as mobile stations such as with portable workstations equipped for field use) are set with password protection so that the computer may not be accessed without the proper password.

- All workstations are set up to go "inactive" after a set time period so that if the staff member leaves the workstation and forgets to logout and shut down, access will not be permitted without the proper password.

- Procedures are established for each work area, depending on the nature of the work area to limit viewing of workstation device screens to only those operating the workstation wherever possible.

- For example, in office areas, all screens should be pointed away from hallways and open areas. The screens should be pointed away from chairs or other locations in the office where unauthorized persons, such as patients, may sit within that office.

- In field operations, ambulance personnel will need to follow procedures to ensure that the workstation device is not left in an open area, such as a countertop in the Emergency Department.

- Workstations will be set so that staff members may not inadvertently change or disable security settings, or access areas of the information system they are not authorized to access.

- Only those authorized to access and use the workstation will be permitted to use the workstation.

- No software may be downloaded or installed on the workstation in any manner without prior authorization. (This prohibition includes computer games, screen savers, and anti-virus or anti-spam programs)

- All staff members will "log off" the workstation whenever it is left unattended.

- All portable workstation devices including laptops will be physically secured wherever possible when not in use.

- Use of any dial up modems and remote access software to access the information system off site must be approved by the Privacy/Information Security Officer.

JORDAN VALLEY EMS AUTHORITY POLICY

POLICY #: 103.4.14 **SUBJECT:** SECURITY OF PHI

CAAS STANDARD: 103.4 **SCOPE:** ALL

Device and Media Controls

The Authority carefully monitors and regulates the receipt and removal of hardware and electronic media that contain e-PHI, PHI and other patient and business information into and out of our stations and other facilities. These controls pertain to the movement, re-use, or disposal of hardware and media within Authority facilities.

As a general rule, simple deletion of files or folders is not sufficient to ensure removal of the file or data. This simply removes the directional "pointers" that allow a user to find the file or folder more readily. Deleted files area usually completely retrievable with special software and computer system expertise.

Disposal. The Authority has in place procedures governing the disposal of hardware and electronic media:

- Sanitizing Hard Disk Drives. All hard disk drives that have been approved by the Privacy/Information Security Officer for removal and disposal (or taken out of active use) shall be sanitized so that all programs and data have been removed from the drive. The Authority will follow industry best practices (such as the U.S. Department of Defense clearing and sanitizing standard – DoD 5220.22-M) when cleaning off hard drives.

- Proper sanitizing usually involves a reformatting of the hard drive in a secure manner with an approved wipeout utility program. Degaussing software may need to be used to ensure total removal of files.

- No hard drive will be reissued, sold or otherwise discarded until the drive has been sanitized.

- Media Re-Use. All e-PHI and other patient and business information shall be removed from any media devices before they are made available for reuse.

- Accountability. The Authority tracks the movement of all computer hardware, workstations, and data storage devices. Movement both within the organization and outside the organization is tracked. A logbook is maintained to record the movement of all hardware and electronic media that is sanitized, reissued, or backed up and stored. The IT Manager or Information Security Officer oversees this accountability log.

POLICY HISTORY:
Implemented February 1, 2015