JORDAN VALLEY EMS AUTHORITY POLICY

POLICY #: 103.4.11 **SUBJECT:** ACCESS TO INFORMATION AND PHI

CAAS STANDARD: 103.4 **SCOPE:** ALL

PURPOSE:
The Authority has established this policy to ensure that all staff members have appropriate access to e-PHI and PHI, and that his or her identity is properly verified before such access can be attempted. This policy also addresses procedures to prevent staff members and former staff members who should not have access to e-PHI and PHI from obtaining it, and for emergency access to the information system.

POLICY:
This policy applies to all the Authority staff members who utilize the electronic information system. It covers key provisions concerning who may have access to e-PHI and PHI, the level of access they may have, protections to ensure proper user identification for access, and emergency access to e-PHI and PHI. This policy also addresses the steps to be followed to terminate access to e-PHI and PHI when a staff member's authorization to access has ended, such as when employment or membership is terminated.

PROCEDURE:
Person or Identify Authorization
To ensure that all individuals or entities that access e-PHI have been appropriately authenticated, the following procedures are established:

- Staff members seeking access to any network, system, or application that contains e-PHI must satisfy a user authentication mechanism such as a unique user identification and password, biometric input, or a user identification smart card to verify their authenticity.
- Staff members seeking access to any network, system, or application must not misrepresent themselves by using another person's User ID and password, smart card, or other authentication information.
- Workforce members are not permitted to allow other persons or entities to use their Unique User ID and password, smart card, or other authentication information.
- A reasonable effort must be made to verify the authenticity of the receiving person or entity prior to transmitting e-PHI.

Security Unique User Identification
To uniquely identify and track one user or workforce member from all others, for the purpose of access control to all networks, systems, and applications that contain e-PHI, and the monitoring of access to the aforementioned networks, systems, and applications, the following procedures are established:

- Any staff member or authorized user that requires access to any network, system, or application that access, transmits, receives, or stores e-PHI, must be provided with a Unique User Identification Number.
- When requesting access to any network, system, or application that access, transmits, receives, or stores e-PHI, a staff member or authorized user must supply their previously assigned Unique User Identification in conjunction with a secure password.
- Staff members or authorized users must not allow anyone else to use their Unique User Identification or password.
- Staff members and authorized users must ensure that their User Identification is not documented, written, or otherwise exposed in an insecure manner.
- Staff members and authorized users must take all reasonable steps to ensure that their assigned User Identification is appropriately protected and only used for legitimate access to networks, systems, or applications.

- If a staff member or authorized user believes their User Identification has been comprised, they must report that security incident to the appropriate supervisor or the Information Security Officer.

Security Password Management
To ensure that passwords created and used by The Authority to access any network, system, or application used to access, transmit, receive, or store e-PHI is properly safeguarded the following procedures are established:

- All staff members who access networks, systems, or applications used to access, transmit, receive, or store e-PHI must be supplied with a Unique User Identification and password to access e-PHI.
- All staff members must supply a password in conjunction with their Unique User Identification to gain access to any application or database system used to create, transmit, receive, or store e-PHI.
- A generic User Identification and password may be utilized for access to shared or common area workstations so long as the login provides no access to e-PHI. An additional Unique User Identification and password must be supplied to access applications and database systems containing e-PHI.
- All passwords used to gain access to any network, system, or application used to access, transmit, receive, or store e-PHI must be of sufficient complexity to ensure that it is not easily guessable.
- Managers of networks, systems, or applications used to access, transmit, receive, or store e-PHI, must ensure that passwords set by staff members meet the minimum level of complexity described in this policy.
- Managers of networks, systems, or applications used to access, transmit, receive, or store e-PHI are responsible for educating staff members about all password related policies and procedures, and any changes to those policies and procedures.
- Password “aging times” (i.e., the period of time a password may be used before it must be changed) may be implemented in a manner commensurate with the criticality and sensitivity of the e-PHI contained within each network, system, application or database.

- Staff members are responsible for the proper use and protection of their passwords and must adhere to the following guidelines:
    - Passwords are only to be used for legitimate access to networks, systems, or applications.
    - Passwords must not be disclosed to other staff members or individuals.
    - Staff members must not allow other staff members or individuals to use their password.
    - Passwords must not be written down, posted, or exposed in an insecure manner such as on a notepad or posted on the workstation.

Security Password Structure
To ensure that all passwords used to control access to any network, system, application, media or file containing e-PHI are secure and not easily guessed, the following procedures are established:

- Passwords should not include easily guessed information such as personal information, names, pets, birth dates, etc.
- If a system does not support the minimum structure and complexity as detailed in this policy, one of the following procedures should be implemented:

- The password assigned should be adequately complex to ensure that it is not easily guessed. If an alternative password structure must be implemented, the complexity of the chosen alternative must be defined and documented.
- If feasible, the current system can be upgraded to support the minimum HIPAA Security Password Structure.
- If feasible all e-PHI should be removed and relocated to a system that supports the minimum HIPAA Security Password Structure.

Emergency Access to e-PHI and PHI

To ensure that access to critical e-PHI is maintained during an emergency situation, the following emergency access procedures are established: If a system contains e-PHI used to provide patient treatment, and the denial or strict access to that e-PHI could inhibit or negatively affect patient care, staff members responsible for electronic information systems must ensure that access to that system is made available to any caregiver in case of an emergency.

Termination of Access

To ensure that access to the information system and e-PHI is terminated when a staff no longer has authorization for access, the following procedure is established. This procedure also applies to terminations in employment or membership in the organization, retirement, resignation, leave of absence, or transfer to an area in the organization where the staff member is no longer authorized to access the information system.

- All supervisors will immediately notify the Privacy/Information Security Officer or and the information system administrator when a staff member has been separated from service with the Authority or when the person no longer is permitted access to the system.
- The staff member's access to the information system will immediately be disabled on the effective date of the separation or, if still on the staff, the effective date when authorization for access has ended.
- The staff member will be removed from all information system access lists.
- The staff member will be removed from all user accounts.
- The staff member will turn in all keys, tokens, or access cards that allow access to the information system.

POLICY HISTORY:
Implemented February 1, 2015