JORDAN VALLEY EMS AUTHORITY POLICY

POLICY #:	103.4.4	**SUBJECT:**	INFORMATION SECURITY GENERAL POLICY
CAAS STANDARD:	103.4	**SCOPE:**	ALL EMPLOYEES AND VOLUNTEERS

PURPOSE:
This policy sets forth our commitment to compliance with those standards established by the Department of Health and Human Services under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") regarding the use and disclosure of Protected Health Information ("PHI") under the Privacy Regulations ("Privacy Rule") and the security of Electronic Protected Health Information ("e-PHI") under the Security Regulations (the "Security Rule"). This policy and our procedures as to the creation, use, disclosure, and security of PHI and e-PHI also applies to other essential patient information, billing and business information, and confidential information that is stored electronically or in any other manner, including paper or hard copy form.

POLICY:
This Policy addresses our general approach to compliance with the Security Rule. As a covered entity under the Security Rule, the company is required to:

1. Ensure the confidentiality, integrity and availability of all PHI and e-PHI the Authority creates, receives, maintains or transmits;
2. protect against any reasonably anticipated threats or hazards to the security or integrity of such information;
3. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required; and
4. Ensure compliance with the Privacy and Security Rule by our staff.

Compliance with the Privacy and Security Rules will require the company to implement:

- Administrative Safeguards--actions, policies and procedures to manage the selection, development, implementation and maintenance of security measures to protect PHI and e-PHI and to manage the conduct of our staff in relation to the protection of and authorized access to patient information.
- Physical Safeguards--physical measures, policies and procedures to protect our electronic information systems, related buildings and equipment from natural and environmental hazards and unauthorized intrusion.
- Technical Safeguards--the technologies and the policies and procedures for its use that protect PHI and e-PHI and control access.

PROCEDURE:
Information Security Officer
The Authority has designated a Privacy/Information Security Officer with overall responsibility for the development and implementation of policies that conform to the Privacy Rule ("Privacy Policies") and the Security Rule ("Security Policies"). The Information Security Officer is responsible for ensuring that The Authority: (i) complies with the HIPAA Security Policies, (ii) develops and implements HIPAA security procedures ("Security Procedures") for each Security Policy, (iii) maintains the confidentiality of all e-PHI created or received by The Authority (as well as other essential patient information, billing and business information, and confidential information that is stored electronically) from the date the information is created or received until it is destroyed, and (iv) trains all staff members of The Authority at the appropriate level of HIPAA training as determined by the Information Security Officer and Privacy Officer.

Implementation of Security Measures
The Authority will implement any security measure that allows it to reasonably and appropriately comply with a specific security standard in the Security Rule. In determining which security measures to implement, the Authority will take into account its size, complexity and capabilities; technical infrastructure; hardware and software security capabilities; the costs of the security measures; and the probability and criticality of potential risks to e-PHI.

JORDAN VALLEY EMS AUTHORITY POLICY

POLICY #:	103.4.4	**SUBJECT:**	INFORMATION SECURITY GENERAL POLICY
CAAS STANDARD:	103.4	**SCOPE:**	ALL EMPLOYEES AND VOLUNTEERS

The Authority will determine what security measures *must* be implemented and will determine those measures that we have *discretion* to implement. The determination as to what security measures are required or discretionary will be reviewed by the Privacy/Information Security Officer to ensure compliance with the Security Rule.

Security Complaints
The Information Security Officer shall be responsible for facilitating a process of individuals (including staff members) to file a complaint regarding our Security Policies or the manner in which e-PHI and other confidential information is handled. The Information Security Officer is responsible for ensuring that the complaint and its disposition are appropriately documented and handled.

Mitigation, Sanctions and Non-Retaliation
The Authority will ensure it mitigates damages that may occur as a result of any violation of the Security Rule or our Security Policies or specific Security Procedures. Any staff members who violate the Security Rule or Authority policies with respect to e-PHI and other protected and confidential information will be disciplined accordingly. This may include verbal or written counseling, suspension, or even termination, depending upon the seriousness of the infraction.

The Authority will not intimidate or retaliate against any person for exercising his or her rights under the Security Rule or for reporting any concern, issue or practice that the person believes in good faith to be in violation of the Security Rule or our Security Policies or specific Security Procedures. The Authority will not require any person to inappropriately waive any rights that person may have to file a complaint with the Department of Health and Human Services.

Security Policies and Procedures
The Authority Security Policies and Security Procedures are designed to ensure compliance with the Security Rule. These Security Policies and Security Procedures will be kept current and in compliance with any changes in the law or regulations. There will be periodic evaluation of our Security Policies and Procedures whenever there are significant changes in the law or regulations or at least on an annual basis when there are no such changes.

Responsibility of All Staff Members
The Authority takes privacy issues very seriously, especially in light of the unique work that we do in EMS and medical transportation. We will only recruit, hire, or accept staff members who are sensitive to patient privacy and who demonstrate a commitment to the principles of protecting our patient information and our business and other confidential information. Every member of the Authority staff is responsible for being aware of, and complying with, the Privacy Rule, the Security Rule, and our Privacy and Security Policies and Procedures. This is an essential requirement of all positions within the organization.

Supervision of Staff Members Who Work With e-PHI
All staff members who use, access or work with e-PHI shall be supervised by appropriate members of management in accordance with their level of e-PHI access. The use of e-PHI by field providers will be supervised by the appropriate field/operations supervisory personnel and/or line officers as appropriate.

POLICY HISTORY:
Implemented February 1, 2015