Mobile Privacy Policy

Athena GTX, Inc. (Athena), hereby acknowledges our duty and responsibility to protect the privacy and security of Individually Identifiable Health Information ("IIHI") generally, and Protected Health Information ("PHI") as defined in the HIPAA Regulations, under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under principles of general and professional ethics. Athena also acknowledges the timely and unimpeded flow of health information for lawful and appropriate purposes.

Definitions

TERM	DEFINITION
ADMS	Athena Device Management Suite
AGENT	An instance of ADMS which is used to receive information directly from a medical monitor. May be referred to as "client"
EPHI	Electronic Personal Heath Information
HIPAA	Health Insurance Portability and Accountability Act of 1996
HITECH	Health Information Technology for Economic and Clinical Health
IIHI	Individually Identifiable Health Information
MANAGER	An instance of ADMS which is used to receive and send data from one or more agent systems. Also known as "Server"
MINIMUM NECESSARY STANDARD	Limit PHI to the minimum needed to accomplish the intended purpose of the use, disclosure or request
PHI	Patient Health Information
RESPONSIBLE ORGANIZATION (RO)	The medical organization managing the product's use in the medical setting.

Collection of personal information

ADMS Manager collects a patient's vital information through medical devices attached to the patient. These vitals can be viewed by medical professionals with access to an instance of ADMS on the same network.

ADMS Manager only saves data on the PC running ADMS Manager. A RO's instance of ADMS and the saved ePHI can only be accessed through the network connected to the ADMS Manager. Therefore, no Athena employee will have access to a RO's instance of ADMS and the saved ePHI without the RO's express invitation.

ADMS does not collect personal information about its users unless voluntarily provided. To wit, Athena will use user information for, but not limited to, communicating with users in relation to services and/or products users have requested from Athena.

5900 NW 86th STREET • SUITE 300 • JOHNSTON, IA 50131 • 515.288.3360 • ATHENAGTX.COM

Transmitting ePHI

Athena is responsible for implementing electronic mechanisms to corroborate that the ePHI has not been altered or destroyed in an unauthorized manner during transmission. All data in transit is encrypted and all transmitting Agents are authenticated with the manager before any transaction.

Storing ePHI

Athena is responsible for implementing electronic mechanisms that ensure the integrity and privacy of stored information. All stored patient data is encrypted and only stored on ADMS Manager. No ePHI is stored on an ADMS Agent. All users must be authenticated within ADMS to view ePHI.

Contact Athena for more information on HIPAA compliance and cybersecurity measures.

Use and Distribution of ePHI

ADMS Manager only saves data on the PC running ADMS Manager. A RO's instance of ADMS and the saved ePHI can only be accessed through the network connected to the ADMS Manager. Therefore, no Athena employee will have access to a RO's instance of ADMS and the saved ePHI without the RO's express invitation. Therefore, Athena does not sell, rent, or lease its customer's information of any kind to third parties at any time or for any reason.

A RO may request an EHR plugin that allows ADMS to transmit patient data to the RO's EHR system.

Responsibilities of the Responsible Organization

Security Management

[1] The RO is responsible for conducting an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by the RO.

[2] The RO is responsible for implementing and enforcing procedures that apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the RO.

[3] The RO is responsible for implementing and enforcing procedures to regularly review various indicators and records of information system activity.

Workforce Security

[1] The RO is responsible for implementing and enforcing procedures for the authorization and/or supervision of workforce members who work with ePHI or in locations where it might be accessed.

[2] The RO is responsible for implementing and enforcing procedures to determine that the access of a workforce member to ePHI is appropriate

[3] The RO is responsible for implementing and enforcing procedures for terminating access to electronic protected health.

Information Access Management

[1] The RO is responsible for implementing and enforcing policies and procedures for granting access to ADMS and its related ePHI, for example, through access to a workstation, transaction, program, process, or other mechanism.

[2] The RO is responsible for implementing and enforcing policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process

[3] The RO is responsible for implementing and enforcing a policy that governs the use of mobile devices that can access, use, transmit, or store ePHI in accordance with HIPAA requirements at 45 CFR Parts 160 and 164, as amended.

Security Awareness and Training

[1] The RO is responsible for implementing and enforcing procedures for periodic security updates

[2] The RO is responsible for implementing and enforcing procedures for guarding against, detecting, and reporting malicious software.

[3] The RO is responsible for implementing and enforcing procedures for monitoring log-in attempts and reporting discrepancies.

[4] The RO is responsible for implementing and enforcing policies and procedures for creating, changing and safeguarding passwords.

Security Incident Procedures

[1] The RO is responsible for:

a. Implementing and enforcing policies and procedures for reporting any suspected or known security incidents to Athena.
b. Make an immediate report of a breach to Athena.
c. Classify severity of the security incident and determine risk to ePHI.

Contingency Plan

[1] The RO is responsible for implementing and enforcing policies and procedures that establish and implement procedures to create and maintain retrievable exact copies of ePHI.

[2] The RO is responsible for establishing (and implementing as needed) procedures to restore any loss of data.

[3] The RO is responsible for defining what constitutes as an emergency as well as implementing and enforcing policies and procedures that establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of ePHI while operating in emergency mode.

[4] The RO is responsible for implementing and enforcing procedures for periodic testing and revision of contingency plans.

[5] The RO is responsible for implementing and enforcing procedures assessing the relative criticality of specific applications and data in support of other contingency plan components.

Facility Access Controls

[1] The RO is responsible for establishing (and implementing as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.

5900 NW 86th STREET • SUITE 300 • JOHNSTON, IA 50131 • 515.288.3360 • ATHENAGTX.COM

[2] The RO is responsible for implementing and enforcing procedures that implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

[3] The RO is responsible for implementing and enforcing procedures that implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.

[4] The RO is responsible for implementing and enforcing policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).

Workstation Use

[1] The RO is responsible for implementing and enforcing policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access ePHI.

Workstation Security

[1] The RO is responsible for implementing and enforcing physical safeguards for all workstations that access ePHI, to restrict access to authorized users.

Device and Media Controls

[1] The RO is responsible for implementing and enforcing policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.

[2] The RO is responsible for maintaining a record of the movements of hardware and electronic media and any person responsible therefore.

[3] The RO is responsible for maintaining a record of the movements of hardware and electronic media and any person responsible therefore.

Access Control

[1] The RO is responsible for implementing regulations pertaining to emergency access procedures.

Audit Controls

[1] The RO is responsible for implementing and enforcing hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.

HIPAA Training Policy

[1] The RO is responsible for implementing a HIPAA Training Policy with all employees with access to ePHI.

Changes to this statement

Athena reserves the right to change this Privacy Policy from time to time. Athena will notify users about significant changes in the way we treat personal information. The continued use of ADMS after such modifications will constitute the user's acknowledgement and consent of the new policy.

5900 NW 86th STREET • SUITE 300 • JOHNSTON, IA 50131 • 515.288.3360 • ATHENAGTX.COM