advantage
ANYWHERE

Advantage Anywhere HIPAA Compliance Statement

Genesis Global Technologies, authors of Occupancy Advantage, submits this statement of policy regarding HIPAA regulations and obligations. While HIPAA compliance is in part dependent on technology, HIPAA compliance is an overall organizational obligation that focuses on your procedural standards and procedural integrity. Therefore, HIPAA compliance for software requires a combination of secure/private technology and compliant business practices. Advantage Anywhere provides clients with a software tool that is HIPAA compliant from a technology standpoint as detailed below. However, Advantage Anywhere technology is only half of the inquiry – how client users use Advantage Anywhere software within their organization must also be addressed.

What is HIPAA?

The Health Insurance Portability and Accountability Act became law in August 1996.
Known as HIPAA, it was designed to set in motion a series of widespread measures focusing on simplifying the processing and distribution of medical information, improving the portability of health Insurance, giving patients access to medical information, and protecting patient data that is stored, processed, or transmitted across public networks.

What's a "HIPAA-compliant" Web App?

A Web App that is "HIPAA-compliant" is one that provides the physical and technological security measures required to ensure that any patient information and other sensitive information remains secure, confidential and unable to be digitally intercepted or otherwise accessed by outside parties. In short, a "HIPPA-compliant" Web App means all required steps have been taken to keep private information private.

Is Advantage Anywhere web app "safe?"

Advantage Anywhere provides a HIPAA compliant version –upon request. We have ensured the Advantage Anywhere web based service complies with all current HIPAA guidelines. We are pleased to reassure people that its Internet security measures are continually updated and monitored and that all transactions are protected and safe.

NOTE: Secure pages (https:) will display a "lock" on your browser window, indicating that all the information submitted through that page is encrypted and protected.

How is the information protected?

There are a number of ways that we ensure the security of your information.

Encryption. We exercise great care in providing secure transmission of your information from your computer to our servers. When you transmit personal information to us, we encrypt it using Secure Socket Layer (128 bit SSL), the industry-standard encryption technology.

Encryption provides a secure means to protect your information as it passes over the Web to our servers.

Firewalls. Our servers and other technical infrastructure are protected from network intrusion using firewalls and other means.

Internal Access. Our employees and contractors have occasional, legitimate needs to access our data servers for purposes of system troubleshooting and maintenance. We ensure that such access is granted only to those who have such needs. All such individuals have signed confidentiality agreements and are continually made aware of their obligations regarding user information. Access is controlled via pre-assigned user accounts that require multiple levels of authentication. All staff members are regularly trained regarding security protection and HIPAA updates.

Physical Site Security. The Hosting Vendor facilities that house our servers, network devices, backup data storage media, and other equipment and information are physically secured and attended. Access is strictly limited to only those individuals who require it for a legitimate purpose. Backups are stored in a HIPAA compliant facility. A BAA Agreement is available.

Policies and Procedures. We continuously evolve and update our internal information security policies and our business continuity and disaster recovery plans. We perform risk assessment, security audit, and system-test activities on an ongoing basis. Our employees and contractors receive frequent training and/or reminders regarding information security and protecting the confidentiality of your information.

Standards and Regulations. We are committed to meet or exceed regulatory and industry self-regulatory guidelines regarding privacy, confidentiality, and information security. On an ongoing basis, we will review and adapt to statutes, regulations, formal private-sector standards, and informal policy guidelines as they apply. In particular, we will comply with all applicable provisions of the Health Insurance Portability and Accountability Act (HIPAA) rules for information security as those take effect.

HIPAA Measures. Advantage Anywhere does not leave data on mobile or stationary devices. Advantage Anywhere does not store passwords on mobile or stationary devices. For the purposes of tracking we require a unique login for each user. As such, we keep a login history and audit trail logs of all activity by user.

Advantage Anywhere generally does not have a direct relationship with individuals whose personal data is submitted by customers to the Advantage Anywhere web app as customer data. Advantage Anywhere does not collect personal information on behalf of our customers, and Advantage Anywhere does not determine how our customers use such data.

User Level Measures. When you register with us, your personal information is password protected, so only you have access to it. It is your responsibility to ensure the security of your

User ID and password. We enforce the use of Strong passwords. We require password changes every 30 days – with no repeat use of passwords. Idle sessions will time out in 15 minutes of no activity and log out the user. The log out applies to all open sessions – regardless of the devices.

Any exceptions or deviations to our HIPAA standards require a signed Request For Exception by the client organization.

Security. Advantage Anywhere maintains appropriate administrative, physical, and technical safeguards to help protect the security, confidentiality, and integrity of data our customers submit to the Advantage Anywhere service as customer data. Advantage Anywhere customers are responsible for ensuring the security of their customer data in their use of the service.