

Privacy Policy

Ahcglobal, Inc. dba/Accessible Home Health Care: dba/Accessible RCM

Last Updated: July 14, 2026

1. Applicability

This Privacy Policy and Security Statement (“Statement”) applies to this Website (“Site”), which is owned and operated by Ahcglobal, Inc./Accessible Remote Care Management . (“Accessible” or “we”) for the purpose of providing information about certain products and services offered by the companies represented on this Site (“Sellers”). Accessible may operate other Websites that are governed by different privacy policies and security statements. This Statement supplements Accessible’s Terms of Use, and is incorporated into such Terms of Use. In the event of any conflict between the Terms of Use and this Statement, this Statement shall control.

2. General

We recognize that privacy and security are a concern for most individuals accessing the Internet. Whether you are buying one of the quality products or services offered on this Site, or just browsing our Site, we want to make you comfortable with our privacy practices and the security measures we take to protect your personal information. By visiting and by using our Site, you agree to be bound by the terms and conditions of this Statement as currently in effect. If you do not agree please do not access or use our Site. If we decide to change this Statement, the changes will be posted here on the Site, so please check back periodically to ensure you have the most current policy. Your continued use of this website will mean that you accept any changes to this Statement.

3. Personal Information

This Statement applies only to personal information collected and stored from users of our Site. Information submitted solely in a business capacity is not covered by this Statement. “Personal information” is information about a natural person that identifies a specific individual, including, but not limited to, his or her name, title, company, physical and electronic addresses, and telephone and fax numbers. A domain name or Internet Protocol address is not considered personal information.

4. Information Collected

If You Only Visit: If you do nothing during your visit to this Site but browse or download information, we automatically collect and store the following information about your visit:

- The Internet Protocol address and domain name used, but not the email address.
- The Internet Protocol address is a numerical identifier assigned either to your Internet service provider or directly to your computer. We use the Internet Protocol Address to direct Internet traffic to you and generate statistics used in the management of this site;
- The type of browser and operating system you used;
- The date and time you visited this Site;
- The web pages or services you accessed at this Site;
- The web site you visited prior to coming to this web site;
- The web site you visit as you leave this web site; and,
- If you downloaded a form, the form that was downloaded.

This information does not identify you personally and is used for gathering web site statistics. Our web site logs do not identify a visitor by personal information.

If You Send Us an EMail: You may choose to provide us with personal information, for example, in an email to Accessible with a comment or question. We use the information provided to improve our service to you or to respond to your request.

Distribution List: The Site will offer you the option of adding your name and email address to a distribution list for information on new products and services, special offers and other marketing opportunities. We will not add your name and email address to such a list unless you affirmatively permit us to do so, that is, you have “opted-in.” You may also remove your name and email address from a distribution list at any time by using the “unsubscribe” technique found in the e-mail message, that is, you may “opt-out” at any time. We will act on your opt-out promptly, but it may not be effective immediately due to normal processing delays.

5. Sharing with Third Parties

Except as outlined below in this Statement, we never provide your personal information to third parties without your consent.

We may provide personal information from a customer to a third party, including a Seller, as necessary to process that customer’s request or order or otherwise service a customer’s account.

We reserve the right to disclose or report personal information in limited circumstances where we believe in good faith that disclosure is required under law, to cooperate with regulators or law enforcement authorities, and to protect our rights or property. This may include the exchange of information with other organizations for fraud protection and credit risk reduction.

We reserve the right to use your e-mail or other address to send you important information relating to your account.

The Site may also contain optional surveys and questionnaires asking for information, as well as several opportunities for visitors to ask questions. We use the information you provide to help us design and build better products, to customize your shopping experience, and to provide advice and purchase recommendations. Taking part in any of these segments is always optional. We do not share the names and e-mail addresses of recipients of our distribution list or the results of our surveys and questionnaires with third parties, including Sellers.

We do research on our users' demographics, interests, and behavior based on the information provided to us when making a purchase, from surveys and from our server log files. We do this to better understand and serve our Users. This research is compiled and analyzed on an aggregated basis so as to prevent identification of personal information relating to any one individual. We may share this aggregated data with our Sellers and other business partners. In addition, we will share aggregated data with our Sellers in order to collect funds owed to us by the Sellers and in order to administer our relationships with those Sellers.

In addition, we may disclose information about you if we have a good faith belief that we are required to do so by law or legal process, to respond to claims, or to protect the rights, property or safety of Accessible or others.

6. Cookies

When you come into our Site, our server attaches a small text file to your hard drive — a cookie. A “cookie” assigns you a unique identifier so that we can recognize you each time you re-enter our Site, so we can recall where you've previously been on our site, and which keeps track of the pages you view on our Site. Cookies help us deliver a better Site experience to our users.

This information collected by using a cookie is sometimes called “clickstream.” We use this information to understand how our users navigate our Site, and to determine common traffic patterns, including what site the user came from. We may use this information to make site navigation and product recommendations, and to help redesign our Site in order to make your experience on our Site more efficient and enjoyable. We may also use this information to better personalize the content, banner ads, and promotions that you and other users will see.

You also have choices with respect to cookies. By modifying your browser preferences, you have the choice to accept all cookies, to be notified when a cookie is set, or to reject all cookies. If you choose to reject all cookies you will be unable to use those services or engage in activities that require the placement of cookies. Certain aspects of the Site may not function properly if

you set your browser to reject all cookies.

7. Security

This Site uses Secure Sockets Layer (SSL) encryption technology. The SSL protocol provides server authentication, data integrity, and privacy on the Web. SSL encrypts your personal and financial information as it is being transmitted, including credit card information, and also verifies the identity of the server and that the original message arrives at its destination.

No data transmission over the Internet can be guaranteed to be 100% secure. As a result, while we strive to protect your personal information, we cannot ensure or warrant the security of any information you transmit to us or from this Site, and therefore you use this Site at your own risk. Once we receive your transmission, we use our best effort to ensure its security on our systems. We also cannot be responsible for criminal acts of third parties, such as “hackers,” who may seek to compromise our security measures through unlawful means. Industry-accepted security measures have been integrated into the design, implementation, and day-to-day operation of the Site.

8. Children

This site is intended for use by persons over the age of 13. Accessible does not seek to collect information about children under the age of 13. No information should be submitted to or posted on this Web site by users under 13 years of age. If a child under the age of 13 submits personal information to this Site, we delete the information as soon as we discover it and do not use it for any other purpose. Accessible encourages parents to take an active role in their children’s use of the Internet, and to inform them of the potential dangers of providing information about themselves over the Internet.

Parents who are concerned about their child’s possible unauthorized use of the Site may contact us at info@Accessiblecorp.com.

9. Endorsements and Links to Other Sites

This Site may contain advertising for the purpose of commercial information and hyperlinks to, or web addresses of, the Web sites of other organizations. When you visit such other Web sites, you are no longer on our Site and you are subject to the privacy and security policies of the new site. We do not review these other privacy and security policies and takes no responsibility for them.

10. Prohibitions on Use

Using the Site to transmit any material (by email, instant messaging, posting or otherwise) that, intentionally or unintentionally violates any applicable local, state, national or international law, or any rules or regulations promulgated hereunder is prohibited.

Using this Site to access or to attempt to access the accounts of others or to penetrate or attempt to penetrate security measures of Accessible's or another entities computer software or hardware, electronic communication system, or telecommunication system, whether or not the intrusion results in the corruption or loss of data is prohibited.

Using Accessible to collect or attempt to collect personal information about third parties without their knowledge or consent is prohibited.

11. Violations of the Statement

Accessible maintains active processes to ensure compliance of this Statement, as well as with legal requirements, contractual agreements, and other commitments in the handling of private information. All violations of this Statement will be strictly enforced. Accessible requests that anyone who believes that there is a violation of this Statement direct the information to info@Accessiblecorp.com.

12. EU Safe Harbor Participation

Accessible recognizes that the European Union ("EU") has an "omnibus" data protection regime established pursuant to the European Data Protection Directive (95/46/EC) (the "Directive"). Among other rules, the Directive generally requires "adequate protection" for the transfer of certain individually identifiable data from the EU to Accessible operations in the United States. Accessible accordingly adheres to the requirements of the EU Safe Harbor Privacy Principles published by the US Department of Commerce ("EU Safe Harbor") with respect to certain individually identifiable data received by Accessible in the United States about (a) employees of its subsidiaries and affiliates in the EU ("European Employee Data") and (b) individual customers and officers, directors, shareholders, owners, managers, employees, and other representatives of legal entity customers in the EU ("European Customer Representative Data").

With respect to European Customer Representative Data, Accessible and/or its affiliates may use and otherwise process such data in order to: perform obligations under its or its affiliates agreements with customers and carry out related business functions; and assure compliance with legal obligations and regulations applicable to Accessible and its affiliates operating in the United States and around the world ("Accessible Group"). Accessible may also disclose European Customer Representative Data for these purposes to its affiliates, service providers and data processors, and regulatory, law enforcement, and other authorities in the United States and other jurisdictions where the Accessible Group has operations where permitted by the EU Safe Harbor rules. In addition, Accessible may disclose or otherwise process European Customer Representative Data in the context of any sale or transaction involving all or a portion of the business, or as may be required or permitted by law and/or the Safe Harbor.

With respect to European Employee Data, Accessible and/or its affiliates provide covered employees in the EU with information regarding the data transfers that are covered by Safe Harbor via separate policies and procedures.

Individuals identified in European Customer Representative Data and European Employee Data may contact Accessible's Safe Harbor Privacy Contact identified below with questions and/or to review EU Personal Data that Accessible holds about them. Employees may also contact their local human resources manager with any questions or concerns. Any such covered individual who cannot resolve his/her question directly with Accessible or its affiliate can contact the local data protection authority for further information and assistance.

We have also aligned our Privacy Policy with the EU General Data Protection Regulation (GDPR) which comes into effect on 25th May 2018.

Safe Harbor Privacy Contact:

The head of Ethics & Compliance

- All questions may be directed to SafeHarbor@Accessible.com To learn more about the Safe Harbor program, and to view Accessible's certification, please visit <http://www.export.gov/safeharbor/>.

13. Customer and Citizen Data Rights

You have several rights, as stated within data protection regulations, to the provision of your personal data to Accessible Home Health Care using this website. These include your rights to request that Accessible Home Health Care:

- Confirms what personal data it may hold about you and for what purposes to you •

Change the consent which you have provided in relation to your personal data •

Corrections to any incomplete or inaccurate personal data

- Provides you with a complete copy of your personal data
- Stop processing your personal data
- Permanently erase all your personal data and confirm to you that it has been erased
(there may be reasons why we may be unable to do this)

To contact Accessible Home Health Care regarding your personal data, email info@Accessiblecorp.com.

14. How do we protect your information?

1. Our website is scanned on a regular basis for security holes and known vulnerabilities in order to make your visit to our site as safe as possible.
2. We use regular Malware Scanning.
3. Your personal information is contained behind secured networks and is only accessible by a limited number of persons who have special access rights to such systems, and are required to keep the information confidential.

4. We implement a variety of security measures when a user submits an inquiry to maintain the safety of your personal information.
5. Personal data will be accurate and where necessary, kept up to date.
6. Personal data will not be kept for longer than is necessary.
7. Personal data will not be transferred to a country or territory outside of the European Economic Area (EEA) unless we can be assured there is an adequate level of protection for the rights and freedoms of the data subjects.

15. Digital Communications & Protected Health Information (PHI)

Digital Communication and Your Privacy

At Ahcglobal, Inc. dba/Accessible Home Health Care (AHHC), we prioritize protecting your Protected Health Information (PHI). While modern technology offers many convenient ways to stay in touch, standard digital platforms—including consumer text messaging (SMS), WhatsApp, Apple FaceTime, and non-secure video chat applications—do not meet the strict encryption and security standards required by federal and state healthcare privacy laws.

- **Clinical & Care Communications:** Our staff and caregivers are strictly prohibited from transmitting clinical details, medical records, or sensitive health information via standard, unencrypted personal text messages (SMS), WhatsApp, FaceTime, or other consumer messaging apps.
- **Authorized Channels:** To protect your privacy, all digital clinical communication, virtual care visits, and electronic health exchanges must be conducted through AHHC-authorized, secure, and HIPAA-compliant digital channels and applications.

16. Patient Consent & Right to Request Alternative Communications

Client Requests for Text, WhatsApp, or Video Chat

We recognize that you or your authorized family representatives may prefer the convenience of communicating via standard text messaging, WhatsApp, FaceTime, or other personal digital platforms. Under federal privacy regulations, you have the right to request that we communicate with you using these alternative methods.

If you explicitly request to communicate via an unsecure platform (such as standard text or WhatsApp):

- We will provide you with a clear warning explaining the security risks (such as the risk of third-party interception or unauthorized access on your device).
- We will require your documented, written consent before transmitting any sensitive health or billing information through these unsecured networks.
- You may revoke this consent at any time by contacting our Privacy Officer.

17. Voice over IP (VoIP) and Interactive Telehealth

Voice over IP (VoIP) and Telehealth Security

When you call our offices or participate in remote telehealth consultations, we utilize secure, professional Voice over IP (VoIP) telephone systems and interactive virtual care platforms.

Unlike consumer-grade communication apps, our VoIP and telehealth systems utilize end-to-end encryption, strict user authentication, and access controls to ensure that your voice conversations, video feeds, and any digital transmissions remain entirely confidential and secure.