Your Privacy

Main Street Health Group is strongly committed to protecting your privacy. This Privacy Policy discloses information about the privacy practices for the website you are currently visiting: www.cuhealthgroup.org . At no time does Main Street Health Group sell or provide to other companies your personal information resulting from inquiries to our website. We only use your personal information to help you find and apply for health insurance and complementary products that may be of interest to you, as per our HIPAA compliant Privacy Statement below. We additionally use leading technologies to protect the security and privacy of your personal information.

PRIVACY STATEMENT
These privacy policies and procedures implement our obligation as an insurance agent to protect the "nonpublic personal information" that we create, receive or maintain on consumers or customers. Throughout the policy, we refer to information that can identify you as a specific individual, such as your name, phone number, email address, Social Security number or credit card number, as "personal information." Further, personal information includes any information involving your health or medical history.

1. No use or disclosure: Our staff will not use or disclose nonpublic personal information except as these Privacy Policies & Procedures or our annual privacy practices notice permit, require or as permitted by law.

2. Medical Information Privacy: Our staff will not disclose or share medical or other specified information at any time as defined by law without consent from the consumer/customer. A consumer/customer may at any time revoke their consent to disclose or share information by written notice. We do not sell, trade or give away your personal information to anyone. We do not disclose your personal information to third parties, unless one of the following limited exceptions applies.
Insurance Companies and Licensed Agents. If you submit an application for an insurance product offered by us, then we will disclose your personal information to the applicable insurance company so they may process your application.
Legal Obligations. We may disclose or report your personal information when we believe, in good faith, that the disclosure is required or permitted under law; for example, to cooperate with regulators or law enforcement authorities or to resolve consumer disputes.
Outside of these exceptions, we will not share your personal information with third parties.
We may collect personal information from you on a voluntary basis in the normal course of business in order to process your insurance application and to serve you better. We may use your personal information to get in touch with you when necessary to process your application or to address questions you may have. We gather anonymous information about you for our internal purposes, and we may share this anonymous information with third parties. Anonymous information is any information that does not personally identify you, including aggregate demographic information such as the number of visitors to our website who link over to us from another website. We use anonymous information primarily for marketing purposes and to improve the services we offer you. We may use "Cookies," "Internet Protocol" addresses or other numeric codes to gather anonymous information. For a more detailed discussion on cookies, please see below.

3. Notice of Privacy Procedures: We will provide an initial and annual Privacy Practices Notice to each customer as required by law and to all consumers before disclosure of any nonpublic personal financial information to nonaffiliated third parties for marketing purposes.
When, if ever, there is a material change to our use or disclosure of nonpublic personal information, nonpublic personal financial information, legal duties, consumers or customers rights or to other privacy practices that render the statements in our notices no longer accurate, we will promptly revise our Privacy Statement to reflect these changes. These notices are available upon request.

4. Opt-out notice: Each customer/consumer will receive their initial privacy practices notice prior to disclosure and or sharing of their nonpublic personal financial information with nonaffiliated third parties for marketing purposes as required by law. Additionally they will receive an opt-out notice a minimum of 30 days, before any sharing or disclosure of nonpublic personal financial information with any nonaffiliated third party as required by law. A consumer may exercise the right to opt-out at any time by completing our opt-out form and returning it to us. We will include the completed opt-out form in the consumer's physical file and make the appropriate notation and changes to their electronic records. We will not share or disclose any customer/consumer nonpublic personal financial information with any person except as allowed under the law or with written consent once we receive a completed opt-out notice.
A consumer/customer may at any time revoke their opt-out by written notice. The revocation will be placed in the consumer/customers physical file and notations made in any electronic records.

5. Distribution of Our Notice: Each consumer/customer will receive his or her initial privacy practices notice no later than the delivery of an insurance policy, service or financial product. Each consumer/customer will receive a notice annually on a date established by us, which reflects our current privacy practices. This annual privacy notice supersedes all prior initial or annual notices.

6. Minimum Necessary Disclosure: We will make reasonable efforts to protect consumer/customer privacy by disclosing or sharing the minimum necessary nonpublic personal information to accomplish the intended function, transaction, or service.

7. Customer / Consumer Rights: We will honor customer's and consumer's rights regarding their nonpublic personal information.
a. Access---We will honor requests in writing to view and copy consumer/customer records that are reasonably identified, reasonably locatable and retrievable. We will within 30 days of receipt of the request, contact the consumer/customer and inform them of the nature and substance of the recorded information and make arrangements for them to view the information and make copies for them for which we will charge $.10 per page plus $10 per hour for staff time.
b. Amendments---Consumers/Customers have the right to request an amendment, correction or deletion to their nonpublic personal information held by us. We will, within 30 days of such request, inform the consumer/customer of our decision to amend, correct, or delete or our decision to not amend, correct or delete. If we decide to amend, correct or delete we will notify the consumer/customer in writing.
c. If we decide not to make any changes the consumer/customer has a right to submit in writing a concise statement setting forth what the consumer/customer thinks is the correct, relevant or fair information and why they disagree with our refusal to amend, correct, or delete nonpublic personal information in their file. Our office will put this statement in the consumer's/customer's file. In the future if we share or disclose any nonpublic personal information from the file we will also furnish a copy of the consumer's/customer's request to amend, correct, delete, our letter informing them of our decision and their response.
The rights granted in this section do not extend to information about the consumer/customer that relates to and is collected in connection with or in reasonable anticipation of a claim or civil or criminal proceeding involving them.

8. Privacy Officer: We will designate one person to be the privacy officer. He or she will have primary responsibility for privacy and security issues. He or she will also be the contact for all complaints involving privacy or security matters.

9. Staff Training: We will train all members of our workforce in these Privacy Policies & Procedures, as needed and appropriate for them to carry out their functions. All members of our workforce will acknowledge in writing within a reasonable time of employment their receipt and training on these Privacy Policies & Procedures.

10. Data Safeguards: We will develop, implement, annually review and maintain reasonable and appropriate administrative, technical and physical safeguards to ensure the integrity and confidentially of the nonpublic personal information we hold and maintain.
a. Physical Access--- We will monitor and ensure that during normal business hours no person is unescorted or unmonitored within the office unless they are an employee or a business associate with whom we have a contract that appropriately limits their use and disclosure of nonpublic personal information held or maintained by us. We will identify, monitor and control who is authorized to posses and who possess keys or the necessary codes for securing and entering the office. Upon any termination of employment keys will be collected and codes changed to maintain the security of the office.
b. Business Associates: We will obtain a contract from all nonaffiliated third parties who will have access to or receive nonpublic personal information in the course of their duties for us. This contract will provide for appropriate safeguards and limit their use and disclosure of the nonpublic personal information we share or disclose to them.
c. Physical Data: We will secure all physical data that contains nonpublic personal information. All files not in use will be filed. No files will be left out of the filing containers over night. All file containers will be secured when the office is closed or not occupied.
d. Electronic Data: We will provide controls on access to and authentication of persons using electronic data. We will install, maintain, and update necessary virus protection, firewall protection and software updates as needed. All employees who must have access to electronic data will have their own unique user ID and unique password. We will ensure that the intentional destruction of data is done using a secure method. Employee training: We will provide annual training on the Privacy Policies and Procedures for protecting the electronic data or form of nonpublic personal information we hold or maintain. We will document the time, date, persons in attendance and subjects covered.

"Cookies"
"Cookies" are small files that are stored by your web browser to help a particular system recognize you and the pages you visited in a website. Our website uses cookies to make your online experience more convenient. We may use data from cookies for a variety of internal purposes, such as studying how users navigate our website. We do not collect any personal information from cookies. Further, no other information we collect from cookies can be linked back to your personal information. Most browsers automatically accept cookies, but if you prefer, you can set yours to refuse cookies. Even without a cookie, you can still use most of the features on our website.

Browsers and Internet Security
Any time you enter or provide personal information in our website, we encrypt it using Secure Socket Layer ("SSL") technology. SSL protects information as it crosses the Internet. To support this technology, you need an SSL-capable browser. Use of a strong encryption, 128-bit browser such as Microsoft's Internet Explorer 4.01 or higher or Netscape Navigator 4.06 or higher is recommended. These browsers will activate SSL automatically whenever you begin shopping for products on our website and when you return to our website to complete an application.

You can tell if you are visiting a secure area within a website by looking at the symbol on the bottom of your browser screen. If you are using Internet Explorer or Netscape Navigator, you will see either a lock or a key. When the padlock is in the locked position, your session connection is taking place via a secure server.
If you need a strong encryption browser, you can go to the Microsoft website or the Netscape website to download the latest Internet Explorer or Navigator browser. We do not recommend the use of beta browser versions.

Security Risk of Using Non-Approved Automated Software Applications
For security reasons to guard the safety of your data, access to this website is limited to SSL-capable browsers such as Microsoft's Internet Explorer 4.01 or higher or Netscape Navigator 4.06 or higher. Under no circumstance should you use any software, program, application or any other device to access or log-in to the www.texasplans.com website, or to automate the

process of obtaining, downloading, transferring or transmitting any content to or from our computer systems, website or proprietary software.

Links to Other Websites
Our website contains links to other websites. Please note that when you click on one of these links you are "clicking" to another website. For Members Only Insurance Services is not responsible for the information, privacy practices or the content of such websites. We encourage you to read the privacy policies of these linked websites as their information privacy practices may differ from ours.