# PRIVACY AND SECURITY POLICY

This Privacy and Security Policy (the "Policy") governs the practices of all Websites (each a "Website" and collectively, the "Websites") that are (1) owned, operated and maintained by Premise Health and its affiliated companies, or (2) operated and maintained for Premise Health by its service providers and other subcontractors. The Website domain is https://myhealthcenterhome.com.

We refer to Premise Health, its affiliated companies, and Premise Health' service providers and other subcontractors in this Policy as "we," "us" or "our." We refer to all applications available through this Website as "Our Applications." Our Applications include, but are not limited to, Patient Portal.

**Personal Information We Collect or Maintain**

When we refer in this Policy to "Personal Information," we mean any information that can be used to identify you and your personal health information. If you register to use Our Applications, we will ask you to provide us with your Personal Information when you register and as our relationship grows. Other Personal Information may be provided by your insurer or other entity that maintains your medical claims history and through eligibility files. Examples of Personal Information include your name, address, health insurance information, social security number, results of your encounters with healthcare providers and drug prescription information. The information will vary depending on which of Our Applications you use.

Your Personal Information will be available for you to access through Our Applications. Any information you provide to Our Applications will also be available for reference by our care managers and your healthcare provider, as applicable. Our Applications and your Personal Information will be stored on computer servers operated by us or by our service providers.

**Cookies**

We collect anonymous, non-personal information about your use of this site through the use of "cookies." Cookies are small bits of information that we transfer to your computer's hard drive that allow us to know how often you visit our Website and the activities you conduct while on our Website (such as the chat rooms you visited). We automatically assign a different cookie to each user. The information collected by cookies helps us generate content and information on web pages specifically designed for you. It also allows us to monitor how many people use this site and for what purpose. We may use cookie information to target certain information to your browser or to determine the popularity of certain content.

Your browser software can be set to reject all cookies. Most browsers offer instructions on how to reset the browser to reject cookies in the “Help” section of the toolbar. If you reject our cookie, certain functions and conveniences of this site may not work properly. We never collect Personal Information through the use of cookies. Our Internal Privacy and Confidentiality Policy We value and respect the privacy and confidentiality of the individuals and organizations that use Our Applications and our Websites and we have placed strict limits on access and disclosure of all Personal Information that is collected and stored in Our Applications. Subject to applicable law, Personal Information is accessed only to maintain and service this Website and Our Applications and to otherwise deliver our services. Furthermore, our internal security measures protect your information against both unauthorized access and misuse by authorized users. (See “Technical Security Measures” below.)

**Access to Your Personal Information**

We will not disclose or provide access to your Personal Information to anyone, unless: (a) we receive your prior consent directly from you or your authorized representative or in the case of children under the age of 13, the child’s parent or guardian, (b) we believe the recipient to be you or your authorized representative, (c) we are required by law to release the information to the recipient; or (d) otherwise so long as such disclosure is permitted by regulations under the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”). To deliver superior service and to quickly identify and resolve technical and other problems, it may be necessary for our employees or authorized agents to access data stored in Our Applications. If access to your Personal Information is necessary to troubleshoot a problem, our employees or authorized agents will explain to our Privacy Officer or his or her designee what data they need to access and explain how they will address the problem. Our internal procedures require these employees and authorized agents to access only the information necessary to correct the problem.

**Confidentiality**

Our employees who are permitted access to your Personal Information have an ethical responsibility not to disclose your Personal Information for any reason. Furthermore, all of our employees, as a condition of employment, are required to sign a confidentiality agreement legally binding them from disclosing any Personal Information with which we are entrusted.

**Notice of Privacy Practices**

Please contact the on-site healthcare facility operated by one of our affiliated companies to receive a copy of the HIPAA Notice of Privacy Practices applicable to such facility.

## Technical Security Measures

**Access to Our Applications**

Authorized users rely on unique user identifications and passwords to access Our Applications. We assign access privileges to Our Applications on a “need-to-know basis” and access by each user is

documented. Please note that you are responsible for taking all reasonable steps to ensure that no unauthorized person has access to your password. We cannot and do not assume any responsibility or liability for the use or misuse by you of the information you transmit or receive while using Our Applications or for the use or misuse of information by third parties to whom you allow access.

**Encryption**

We use Secure Socket Layer ("SSL") encryption technology when transmitting your Personal Information to our servers. SSL helps to ensure the integrity and privacy of your Personal Information during transmission. Encryption involves systematically scrambling numbers and letters, so that even if someone managed to intercept the information, they would not be able to make sense of it. In order to take advantage of this encryption technology, you need to have an Internet browser that will support 128-bit encryption. As an additional security measure, your Personal Information is kept in a database that resides on a server that is physically separate from any other servers at a secure facility.

**Firewall Technology**

Firewalls prevent unauthorized system access and are implemented between the Internet and the servers on which Our Applications reside. Access to Our Applications is not permitted without going through firewalls. We currently use industry standard firewall technology.

**Our Facilities and Physical Security**

Our web-hosting servers operate from a secure, off-site facility. Physical security safeguards are in place to protect against environmental hazards, such as a fire or a flood, and against theft and unauthorized access to the hardware components of our systems. These safeguards include alarm systems, video surveillance and motion detectors in selected areas. We conduct criminal background checks on each individual that is permitted access to our systems.

**Software Discipline**

Software discipline measures are in place to ensure the proper functioning and integrity of the software used to support Our Applications. Antivirus technology is used for virus prevention, detection and removal. Unauthorized software is prohibited from being installed on any system supporting Our Applications.

**Auditing Activities**

Our systems create audit trail logs to proactively monitor activities on our systems. All user information, privileges, and date and time of access, can be audited routinely to ensure adequacy of training and compliance with policy. We can analyze usage patterns and can identify all breaches of information security, leading to corrective action to prevent future occurrences.

**Current Standards and Technologies**

We are committed to meeting or exceeding current information security industry standards and any federal legislation, including HIPAA. We constantly review the latest standards, technologies, and legislation and modify our practices and software accordingly.

**Links to Other Websites, Content Contractors and Their Cookies**

Certain content and services offered to you through this Websites are stored on websites not hosted or operated by us. For your convenience we also provide links to websites that are not operated by us. We refer to such web sites as "Third Party Websites." We do not disclose your Personal Information to Third Party Websites, but you should be aware that any information you disclose once you access these other websites is not subject to this Policy. In addition, Third Party Websites may use their own cookies when you click on their advertisements or link to their website or service. We have no access to, or control over, these cookies. We do not endorse and are not responsible for the privacy practices of any Third Party Website. You should review the privacy policy posted on each Third Party Website to understand how that web site collects and uses Personal Information. Please remember that if you enter a website that does not display the name "Premise" or "Premise Health" you are on a Third Party Website.

**Use of De-Identified Information**

Unless provided otherwise in a binding legal agreement to which we are a party, and only to the extent permitted by the regulations promulgated by the U.S. Department of Health and Human Services under HIPAA, we may at times aggregate de-identified personal information and may compile and distribute statistical analyses and reports utilizing aggregated data derived from this information. We may also share such information with our partners. Any information that can be traced back to an individual, including, for example, name, address, telephone numbers and e-mail addresses, will not be included in the aggregate data.

**Changes to Policy; Contact Information**

Changes to these policies will occur as warranted and will be posted on this page. Please refer to it occasionally to keep up-to-date on our current policies. If you have any question regarding this Policy, if you want to correct any Personal Information that we have collected, or if you feel that we are not abiding by this Policy, you should contact us as follows:

Premise Health
205 Miller Springs Court
Franklin, TN 37064

Last Updated: February 2, 2015