

Effective Date

This Privacy Policy is effective as of January 1, 2019.

Introduction

SPH, LLC dba SimplePay Health and its subcontractors (collectively, "SimplePay", "SimplePay Health", "we", "us" or "our", unless otherwise specified) respect your right to privacy. This Privacy Policy is designed to inform you about how we collect, use and share information about you, including from or through your employer, its health plan and its health plan contractors, in person, by phone, through mail or email or through our website www.simplepayhealth.com, or any other website, mobile sites, mobile applications or social media accounts owned and/or operated by SimplePay or its subcontractors (collectively, our "Sites"). By accessing or using our Sites or otherwise disclosing information to SimplePay, you consent to our collection, use, and sharing of your information in accordance with this Privacy Policy.

In the event of any conflict between the terms of this Privacy Policy and the privacy policy of our subcontractor, the terms of the subcontractor's privacy policy will apply.

Contact Us

If you have questions or complaints regarding this Privacy Policy or our related privacy practices, please contact us at the address below or by calling us at (800) 606-3564 or emailing healthpro@simplepayhealth.com.

SimplePay Health, 12712 Park Central Drive, Suite 100, Dallas, TX 75251, Attn: Privacy Officer

Personal Information

Personally Identifiable Information (or "Personal Information") is information that we collect about you that may be used to identify you, as well as other personal data, including your full social security number or a portion of your social security number. Some of the Personal Information provided by you or collected by us may be health information. Although SimplePay is not a "covered entity" under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), SimplePay is subject to some aspects of HIPAA when SimplePay performs services on behalf of covered entities, including health plans sponsored by employers for their employees. SimplePay is considered a "Business Associate" under HIPAA when providing services to covered entities. We comply with all applicable HIPAA requirements as a Business Associate and hold these HIPAA requirements in the highest regard as a fundamental part of our operating procedures.

We may use Personal Information for a number of purposes such as ...

- Contacting you via the contact information you disclose, e.g. email address

- Ensuring compliance to your employer's health program and sharing appropriate information with your employer and/or employer's authorized vendor
- Linking to your spouse or domestic partner's information
- Responding to a specific request from you
- Administering feedback or surveys
- Providing you with information about our services
- Making context-driven recommendations to you, including proactive recommendations
- Performing analytics to improve our capabilities
- Complying with applicable laws and regulations
- Protecting someone's health, safety, or welfare
- Protecting our rights, the rights of affiliates or related third parties, or taking appropriate legal action
- Keeping a record of our transactions and communications
- As otherwise necessary or useful for us to conduct our business with you and your employer, so long as such use is permitted by law.

The Websites are intended for a United States audience. Any information you provide, including any Personal Information, will be transferred to, processed by, and stored on computer servers located within the United States.

Sharing Information

We will not sell, share, or rent Personal Information that is collected in ways different than from what is disclosed in this Privacy Policy. We will only share your Personal Information with third parties as outlined in this policy and as otherwise permitted by law. We may share Personal Information if all or part of SimplePay is sold, merged, dissolved, acquired, or in a similar transaction. We may share Personal Information to a covered entity that has authorized access to your Personal Information in our role of Business Associate. An example of a covered entity is your employer. We may share Personal Information in response to a court order, subpoena, search warrant, law or regulation. We may cooperate with law enforcement authorities in investigating and prosecuting activities that are illegal, violate our rules, or may be harmful to other visitors. We may also share Personal Information with other third party companies that we collaborate with or hire to perform services on our behalf. For example, we may hire a company to help us send and manage email, and we might provide the company with your email address and certain other information in order for them to send you an email message on our behalf. Similarly, we may hire companies to host or operate some of our websites, related computers, and software applications.

User Tracking

"Non-personal information" means information that does not permit us to specifically identify you by your full name or similar unique identifying information such as a social security number, address, or telephone number. We may use various technologies to gather non-personal information from our Websites' visitors such as which pages are used and how often they are used, and to enable certain features and capabilities. We may use browser "cookies" very minimally and do not store Personal Information in cookie sessions. "Cookies" are small text files that may be placed on your computer when you visit a website or click on a URL. We may use analytics companies to gather information and aggregate data from our visitors such as which pages are visited and how often they are visited, and to enable certain features in our Websites.

Some Personal Information, such as a unique identifier, will be utilized to track user account access, failures, retries, and suspicious activity within your account. This logged activity will not contain Personal Information, but rather activity data within our cybersecurity and security records that map or correlate to your unique person identifier.

Security

We maintain reasonable administrative, technical, and physical safeguards designed to protect your Personal Information. Personal Information is encrypted "at rest" and "in motion" as mandated by HIPAA and is stored in secured locations and on secured server equipment. Access to Personal Information is highly controlled to authorized employees, representatives, or agents and our employees receive compliance and privacy training annually. Secure protocols and technologies are utilized such as encryption, TLS, SSL, cryptography, firewalls, intrusion detection, and more. However, no security system is impenetrable and given the nature of the Internet, we cannot guarantee absolute security, nor can we guarantee that the information you supply will not be intercepted while being transmitted to us over the Internet from your location. We are not liable for the illegal acts of third parties such as criminal hackers. In the event we become aware of a data security breach, we will provide you with notice as required by applicable federal and state laws using contact information we have collected from you. SimplePay employees and our third party service providers must abide by all security, privacy, and compliance policies and those who violate them are subject to corrective action, up to and including termination of employment or other legal action as permitted by law.

Your Obligation

The Websites may contain privileged and confidential health information that is privileged and legally protected from disclosure by federal law, HIPAA. This information is intended only for the use of the individual logged in to the Websites and that is authorized to see your account information. If you are not the intended recipient, user, or have access to an account without expressed and direct permission from the account owner, you are hereby notified that reading, disseminating, disclosing, distributing, copying, acting upon or otherwise using the information contained on any Websites screen is strictly prohibited. If you have access to information or data in error, please notify us immediately and log out of the Websites immediately. As well, you should notify us promptly if you suspect someone has

obtained unauthorized access to your Personal Information. You can contact us at (800) 606-3564 or at healthpro@simplepayhealth.com. If you choose to use the Websites in public, it is your obligation to protect your own information as your screen may be visible to all visitors in the public location. Therefore, please be thoughtful in what you type, enter, or review within the Websites and understand that your Personal Information may become public. We strongly recommend you do not divulge your password to anyone so that others cannot access your Personal Information. We will never ask you for your password in an unsolicited phone call or in an unsolicited email. Our support staff will request verification of your identify before assisting you with your Website accounts. As a recommended practice, you should sign out of the Websites and close your browser window when you have finished using the Websites so others cannot access your Personal Information and correspondence by using your desktop or laptop computer. If you access the Websites through the use of a smartphone or other mobile device, we expect you to use the security controls available on your device (such as setting a confidential password) to prevent unauthorized individuals from accessing your information. We further recommend that you terminate each session to reduce the risk of inappropriate access. If you remain continuously logged in, you assume the risk that unauthorized individuals may be able to access your Personal Information.

Users under the Age of 18

SimplePay does not provide user access or user accounts in the Websites for individuals under 18 years of age. Parents or guardians of children or dependents less than age 18 years of age can maintain Personal Information for their children or dependents in the Websites; as such, this Privacy Policy applies to all Personal Information held in the parent or guardian account whether it is the account owner's Personal Information or a child or dependent's Personal Information.

Our Electronic Communication Practices

We may send electronic communications on a periodic basis using your name, email, and phone number via email, phone call, or text messaging. Correspondingly, we offer you appropriate consent mechanisms for some communications, such as opt-out within the communications themselves. To generally opt-out of online communications, feel free to contact us at (800) 606-3564 or at healthpro@simplepayhealth.com.

Changes to the Privacy Policy

We reserve the right to change the terms of this Privacy Policy, including how Personal Information is utilized. Those changes and any other material changes will be documented within this policy and provided to you on the Websites. You may also request the latest Privacy Policy at healthpro@simplepayhealth.com.