MEDIKEEPER SECURITY STATEMENT

Last Updated: October 2016

THIS RBHS WELLNESS PORTAL IS PROVIDED TO YOU BY HOME SUPPORT SERVICE PTY LTD (HSS) WHO HAS CONTRACTED WITH MEDIKEEPER INC., WHO ARE MANAGING AND OPERATING THIS PORTAL ON BEHALF OF HSS.

About this Security Statement

This MediKeeper Security Statement ('Security Statement') applies to the MediKeeper, Inc. website www.medikeeper.com ("MediKeeper"). Through links provided by MediKeeper, you may be brought to other websites that MediKeeper has partnered with, including companies providing claims and biometric screening data, coaching services, and health content. For the Security Statement of these websites, please refer to the Security Statements available in the websites of our partners.

This Security Statement explains:

Security of your personal information collected and/or processed through MediKeeper; and

Your Obligations as a User of MediKeeper

MediKeeper aims to maintain strict procedures and standards and take all reasonable care to prevent unauthorised access to your personal information, and to protect the security of your personal information during transmission. MediKeeper constantly monitors developments in security and encryption technology and will review and update its processes in line with industry standards.

MediKeeper has taken several security initiatives such as deploying technological hardware and software, policies and procedures, and addressing operational security issues.

1. Security of Personal Information

Personal information supplied by you to MediKeeper shall be used in providing MediKeeper's services under the MediKeeper Terms of Service.

To ensure security, transmission of personal information over the Internet between the browser and the servers in the MediKeeper portal is encrypted using the proven Secure Socket Layer ("SSL") technology, an industry standard security measure available through your browser. Encryption is a mechanism of transmitting data in a secure manner, where the data is encrypted using a key (this key is provided by a recognized Certificate Authority (CA))

All your personal information collected and/or processed by the MediKeeper portal is stored in secured repositories in our secured data center. Only authorized personnel have access to the data repositories in limited circumstances and they are prohibited from making any unauthorised disclosure of your personal data. Backups are performed to ensure that your personal information is safe against system failures. These backups are stored in a secured location.

MediKeeper, in its goal to protect your information, has implemented various security features, including:

1.1. Firewalls and Intrusion Prevention Systems

1.2. Anti-Virus Software

1.3. Internal Policies and Guidelines

1.4. Security Assessments and Surveillance

1.5. Server side Authentication through Digital Certificates

Where relevant, such as in linked online services, additional security features are implemented including:

1.6. Login ID and Password Verification

1.7. Encryption of Passwords

1.8. Account Locking

1.9. Automatic Log out

1.1. Firewalls & Intrusion Prevention Systems

Firewalls act as filters that control and monitor information flowing in or out of a protected network. MediKeeper also has an industry standard Intrusion Prevention System to automatically block known attacks from hackers. The Intrusion Prevention System alerts MediKeeper's security personnel about possible attacks-in-progress and MediKeeper keeps audit logs to provide a trail of information.

1.2. Anti-Virus / Anti-Malware Software

With the outbreak of viruses over the internet, it is critical for MediKeeper to have anti-virus / anti-malware software. MediKeeper has implemented industry standard anti-virus / anti-malware software to ensure its systems are safe from viruses and malwares.

1.3. Internal Policies & Guidelines

MediKeeper adopts various policies and procedures for managing system access, system back-ups and other operations management to safeguard access to MediKeeper's systems. Several guidelines and procedures have been put in place to minimize potential security breaches and to ensure and protect the data integrity of MediKeeper's network.

1.4. Security Assessments and Surveillance

MediKeeper engages security consultants to perform independent regular periodic security assessments on our security infrastructure to detect and to immediately address any currently known high risk vulnerabilities. MediKeeper also engages security consultants for continuous security surveillance to detect and immediately address any abnormal activities.

1.5. Server side Authentication through Digital Certificates

MediKeeper's transaction systems are secured with a digital certificate to enable safe communications with our customers. Such a feature ensures message privacy, web site authentication, and message integrity. You will be able to verify the website identity by clicking on the closed padlock icon located either at the top or bottom of your browser window.

1.6. Login ID and Password Verification

Your Login ID and Password will be used to authenticate you during logins to online services. To ensure the integrity of your Login ID and Password, MediKeeper advises you to periodically change your Password and to keep it secret.

1.7. Encryption of Password

Passwords are treated with the highest level of security. MediKeeper makes use of industry standard technologies to encrypt and protect your Password.

1.8. Account Locking

Invalid login attempts are logged and the account is locked by MediKeeper's system after the allowed login / sign-on attempts are exceeded. Once your account is locked you need to call our Customer Service Center to reactivate your access.

1.9. Automatic Log Out

If there is prolonged inactivity during your logged in online session, MediKeeper's system will automatically log you out of the system. You are then required to re-login.

2. Your obligations as User of MediKeeper Portal

As a user, you play an important role in ensuring the security of your online sessions when using MediKeeper's online services and those services provided through links in the MediKeeper Portal.

2.1. Review your Account Activities

You are advised to regularly review your account activities. If you suspect any unusual account activity, immediately contact MediKeeper using the contact information provided below.

2.2. Maintaining the secrecy of your Login ID and Password

You are responsible for maintaining the secrecy of your Login ID and Password. MediKeeper will not be able to secure your information if you reveal your Login ID and Password to any third party. MediKeeper's personnel are not authorized to ask you for your Password.

2.3. Use strong password

When selecting a password do not associate your selected password with anything personal such as names, birth dates, phone numbers or other familiar words. Do use a combination of numbers, lower and upper case alphabets and special characters, for example *, %, #, ^, &, and a minimum length of 8 characters for your password.

2.4. Log off / Log out

Never leave your computing device unattended during your online transaction session. Always remember to log off or log out after you have completed your online transaction. You are advised to check your last login date and time immediately after you have login / sign-on. If you suspect any unusual account activity, please contact MediKeeper immediately using the contact information provided below.

2.5. Keep your computing device's Operating System (OS) and browser up-to-date

To secure the information transmitted between your computing devices (e.g. a Personal Computer) and MediKeeper's systems, you will need to use a current version of a reputable browser and ensure the security fixes for the computing device and the browser are up-to-date.

2.6. Install Internet security anti-virus / anti-malware software

For you to have safe and secure online transaction sessions, you should ensure that you have installed internet security anti-virus / anti-malware software on your computing devices for added protection.

2.7. Clearing your browser

After the completion of your online transaction, to protect the privacy of your information, you are advised to clear the browser's cache by taking such steps as may be required by your internet browser.

3. Enquiries / Complaints / Communication

Should you have any query / concerns / complaints, in relation to this Security Statement, kindly contact us at:

MediKeeper, Inc.

5930 Cornerstone Court West, Suite 190

San Diego, CA 92121

Customer Service: 1-858-251-3250

E-mail: customerservice@medikeeper.com