



Terms and Conditions

01 January 2016

This Agreement (the “Agreement”) is entered into by and between theHealthSource (Pty) Ltd and the entity agreeing to these terms (“Customer”).

1. ACCEPTABLE USE POLICY

1.1 USER DEFINITION

For the purpose of this agreement, a user is defined as anyone who uses theHealthSource (Pty) Ltd computer, computer network, or uses a computer to access theHealthSource (Pty) Ltd products or services.

A computer system includes, but is not limited to any desktop, laptop, server, mainframe, smartphone, blackberry or cloud computer system.

1.2 SENSITIVE/CONFIDENTIAL INFORMATION DEFINITION

This document refers to “sensitive” and “confidential” information. However it is recognised that there are many occasions where information, whether spoken or written may not have an obvious classification level at the time it is being used.

Users are required to use discretion and common sense to identify information that may be sensitive and to protect it accordingly.

This document explains your obligations to protect sensitive information.

1.3 AGREEMENT

Each time you logon to theHealthSource (Pty) Ltd computer, network, products or services, you agree to be bound by this agreement. You acknowledge that you are accountable to theHealthSource (Pty) Ltd for your actions and that theHealthSource (Pty) Ltd may take legal action for any breach of this agreement. You must not attempt to access theHealthSource (Pty) Ltd computer, network, products or services unless you are authorised to do so.

1.4 ACCOUNTABILITY

In order to access theHealthSource (Pty) Ltd computer, network, products or services, you will be allocated a unique User Account that must be used to logon.

You are accountable for all actions attributable to allocated User Account.

You may be issued a User Account that provides privileged access (e.g. administrator access) to theHealthSource (Pty) Ltd computer, network, products or services.

Privileged access is provided on the condition that the terms of this agreement are still adhered to. Misuse of any privileged account will be taken very seriously.

1.5 ACCOUNT USE

For any User Account, you will not allow another person to share or use this User Account.

You will be required to create a password to protect access to the account.

Your password must comply with the password standard as defined in the Password Policy.

You are responsible for keeping your password secret.

You must not disclose your password either on purpose or accidentally to any other person for any reason except for allowing an authorised theHealthSource (Pty) Ltd computer engineer to access your computer in order to fix a problem.

You must change your password immediately after the engineer has completed their work, or at any other time you suspect that your password may be known by any other person.

1.6 THEHEALTHSOURCE (PTY) LTD DEVICES

You must not make any unauthorised modifications to theHealthSource (Pty) Ltd owned devices. An unauthorised modification includes installing unauthorised software, or disabling computer security software for any reason. If you have cause to install software or modify any settings, you must call the help desk to seek advice and guidance first.

All computer devices issued to you by theHealthSource (Pty) Ltd will remain the property of theHealthSource (Pty) Ltd and must be returned to the company on request.

If you take theHealthSource (Pty) Ltd owned devices away from the agreed areas, it must immediately be reported in writing to theHealthSource (Pty) Ltd.

Any damage to or loss of theHealthSource (Pty) Ltd owned devices must be reported to theHealthSource (Pty) Ltd in writing as soon as you become aware of the damage or loss.

1.7 NON-THEHEALTHSOURCE (PTY) LTD / PRIVATE DEVICES

Highly Restricted and Personal data should not be stored unprotected on a personal device.

Some controls may be enforced which may impact the way you use a personal device. For guidance, each device accessing clinical information must be protected with the following controls where they are available:

- DigitalPersona Fingerprint Reader

Devices must not be modified, sometimes referred to as “chipped” or “jailbroken” to circumvent vendor’s controls.

1.7 MISUSE

Misuse of or attempted misuse of theHealthSource (Pty) Ltd computer, network, products or services can have serious consequences for both theHealthSource (Pty) Ltd and the user concerned.

The use of theHealthSource (Pty) Ltd computer, network, products or services for any of the following reasons would constitute misuse under this agreement. These are to be used as examples and the list is not exhaustive:

- Providing information unless expressly permitted as a function of your job
- For conducting or encouraging activities that may damage the reputation of theHealthSource (Pty) Ltd or its customers.
- Performing activities that could expose company highly restricted or confidential information
- Uploading any theHealthSource (Pty) Ltd software, services or information to unauthorised 3rd party locations including unauthorised internet based file transfer services
- Users must not attempt to access systems or services to which they have not been granted access, probe the systems or services for security weaknesses or compromise systems or services.
- Change or disable the security configurations, anti-virus or other protection or monitoring software on theHealthSource (Pty) Ltd owned devices.
- Bypass or circumvent any security system or install any program or software which has this effect.

Users should contact the theHealthSource (Pty) Ltd help desk for advice if they are unsure of the legitimacy of any action they may wish to undertake.

1.8 PROTECTION OF INFORMATION

You are required to use reasonable measures to ensure the confidentiality of information. This means that you are responsible for ensuring that only authorised individuals have access to any information.

You must use the measures provided by theHealthSource (Pty) Ltd systems and services to protect information.

Some users will have access to sensitive business information and or personal information. This information requires special care.

The following rules should be followed when handling sensitive information:

- E-mail is not necessarily secure. Do not send unprotected sensitive information by email
- Do not set auto forward on for email
- Sensitive data should be encrypted when stored outside of theHealthSource (Pty) Ltd systems and services.
- Sensitive data should be encrypted when sent via e-mail or when stored on removable media.
- Do not read sensitive information where you can easily be overlooked (e.g. where the computer screen is visible to other parties)
- Be aware of your surroundings and do not openly speak about sensitive information where you can easily be overheard

- Do not leave sensitive documents uncollected on printers. Always use secure printing if the service is available.

1.9 REPORTING SECURITY INCIDENTS

It is a requirement that you report any security incident or suspected security incident that you become aware of immediately in writing to theHealthSource (Pty) Ltd.

If you suspect that something you have seen or being asked to do does not comply with this agreement, you must immediately report this in writing to theHealthSource (Pty) Ltd.

You must immediately report the following incidents, or where you suspect this is the case in writing to theHealthSource (Pty) Ltd:

- someone has accessed any theHealthSource (Pty) Ltd software, services or information without authorisation,
- you have lost or suspect you have lost any theHealthSource (Pty) Ltd owned devices,

2. SERVICES

2.1 FACILITIES AND DATA TRANSFER

As part of providing a service, theHealthSource (Pty) Ltd may transfer, store and process Customer data.

By using theHealthSource system, Customer consents to this transfer, processing and storage of Customer Data.

2.2 MODIFICATIONS TO THE SERVICES.

Changes or enhancements will be made to theHealthSource system from time to time.

3. CUSTOMER OBLIGATIONS

3.1 COMPLIANCE

Customer will use theHealthSource system in accordance with the Acceptable Use Policy.

New application features or functionality will be made available from time to time the use of which may be contingent upon Customer's agreement to additional terms.

3.2 UNAUTHORIZED USE

Customer will use commercially reasonable efforts to prevent unauthorized use of the System and Services, and to terminate any unauthorized use.

Customer will promptly notify administrators of theHealthSource system of any unauthorized use of, or access to, the Services of which it becomes aware.

3.3 RESTRICTIONS ON USE

Unless administrators of theHealthSource system specifically agree in writing, Customer will not, and will use commercially reasonable efforts to make sure a third party do not:

- (a) sell, resell, lease or the functional equivalent, the System or Services to a third party (unless expressly authorized in this Agreement);
- (b) attempt to reverse engineer the System, Services or any component;
- (c) attempt to create a substitute or similar system or service through use of, or access to, the System or Services;
- (d) use the System or Services for High Risk Activities; or
- (e) use the System or Services to store or transfer any Customer Data that is controlled for export under Export Control Laws.

Customer is solely responsible for any applicable compliance with HIPAA.

4. SUSPENSION

4.1 SUSPENSION OF END USER ACCOUNTS BY THEHEALTHSOURCE ADMINISTRATORS

If administrators of theHealthSource system become aware of an End User's violation of the Agreement, then administrators of theHealthSource system may terminate the Customer access to its systems and services.

4.2 EMERGENCY SECURITY ISSUES

Notwithstanding the foregoing, if there is an Emergency Security Issue, then administrators of theHealthSource system may automatically suspend the offending use.

5. CONFIDENTIAL INFORMATION

5.1 OBLIGATIONS

Each party will:

- (a) protect the other party's Confidential Information with the same standard of care it uses to protect its own Confidential Information; and
- (b) not disclose the Confidential Information, except to Affiliates, employees and agents who need to know it and who have agreed in writing to keep it confidential.

Each party (and any Affiliates' employees and agents to whom it has disclosed Confidential Information) may use Confidential Information only to exercise rights and fulfil its obligations under this Agreement, while using reasonable care to protect it.

Each party is responsible for any actions of its Affiliates' employees and agents in violation of this Section.

5.2 EXCEPTIONS

Confidential Information does not include information that:

- (a) the recipient of the Confidential Information already knew;
- (b) becomes public through no fault of the recipient;

- (c) was independently developed by the recipient; or
- (d) was rightfully given to the recipient by another party.

5.3 REQUIRED DISCLOSURE

Each party may disclose the other party's Confidential Information when required by law but only after it, if legally permissible:

- (a) uses commercially reasonable efforts to notify the other party; and
- (b) gives the other party the chance to challenge the disclosure.

6. INTELLECTUAL PROPERTY RIGHTS; BRAND FEATURES

6.1 INTELLECTUAL PROPERTY RIGHTS

Except as expressly set forth herein, this Agreement does not grant either party any rights, implied or otherwise, to the other's content or any of the other's intellectual property.

As between the parties, Customer owns all Intellectual Property Rights in Customer Data, and theHealthSource (Pty) Ltd owns all Intellectual Property Rights in the System or Services.

6.2 DISPLAY OF BRAND FEATURES

Customer Brand Features may be displayed in theHealthSource system when so authorized by Customer (such authorization may be provided by the Customer uploading its Brand Features into the Services or other methods).

theHealthSource system may also display theHealthSource Brand Features on the Service Pages.

Neither party may display or use the other party's Brand Features beyond what is allowed in this Agreement without the other party's prior written consent.

6.3 BRAND FEATURES LIMITATION

Any use of a party's Brand Features will inure to the benefit of the party holding Intellectual Property Rights in those Brand Features.

A party may revoke the other party's right to use its Brand Features pursuant to this Agreement with written notice to the other and a reasonable period to stop the use.

7. PUBLICITY

Customer agrees that theHealthSource (Pty) Ltd may include Customer's name or Brand Features in a list of theHealthSource system customers, online or in promotional materials.

Customer also agrees that theHealthSource (Pty) Ltd may verbally reference Customer as a customer of the theHealthSource products or services that are the subject of this Agreement.

This section is subject to Section 6.3 (Brand Features Limitation).

8. REPRESENTATIONS, WARRANTIES AND DISCLAIMERS

8.1 REPRESENTATIONS AND WARRANTIES

Each party represents that it has full power and authority to enter into the Agreement.

Each party warrants that it will comply with all laws and regulations applicable to its provision, or use, of the Services, as applicable (including applicable security breach notification law).

8.2 DISCLAIMERS

TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW, EXCEPT AS EXPRESSLY PROVIDED FOR HEREIN, NEITHER PARTY MAKES ANY OTHER WARRANTY OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, INCLUDING WITHOUT LIMITATION WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR USE AND NONINFRINGEMENT.

9. INDEMNIFICATION

9.1 BY CUSTOMER

Customer will indemnify, defend, and hold harmless theHealthSource (Pty) Ltd, from and against all liabilities, damages, and costs (including settlement costs and reasonable attorneys' fees) arising out of a third party claim:

- (i) regarding Customer Data or Customer Domain Names;
- (ii) that Customer Brand Features infringe or misappropriate any patent, copyright, trade secret or trademark of a third party; or
- (iii) regarding Customer's use of the Services in violation of the Acceptable Use Policy.