Please return to:

HealthOne Access
C/- WellSouth
P O Box 218
Dunedin 9054

Fax: 0800 477 116
Email: it.helpdesk@wellsouth.org.nz

HealthOne ACCESS DEED and Application for Account

BETWEEN

Pegasus Health (Charitable) Ltd - (Pegasus)

AND

Health Care Professional Name_____("you")

This deed is dated the _____ day of _____ 20_____

---

1 Objectives:

Pegasus is the agent of the local District Health Board (DHB) for the management of the HealthOne database described below. The parties wish to enter into this agreement to enable health care professionals to have timely access to patients' health information in order to facilitate the provision of improved health services to those patients. Under this agreement you are granted access to specified patient records provided by participating DHB's, General Practice, Pharmacy and other community organisations (full list available on www.HealthOne.org.nz) using a service referred to as HealthOne. You will be an "authorised user" of HealthOne. This agreement sets out the basis on which such access is provided by organisations who contribute patient data.

2 Medical Information in HealthOne:

Specified medical records are made available via HealthOne to facilitate access to clinical information by those treating the patient. The law authorises the sharing of information between treating providers in a number of circumstances. Healthcare professionals are encouraged to provide information to patients about HealthOne. Patients can choose not to have their information shared via HealthOne if the information was not sourced from that care provider facility, for example this option applies to a community laboratory test ordered by a GP being viewed by a DHB health provider.

3 Authorised User Obligations:

You agree to abide by the following conditions of access at all times:

a) You will only access information from HealthOne for the purpose of providing treatment to patients under your clinical care.

b) Any information that you obtain from HealthOne must be kept confidential and used only for the purposes of providing the above treatment. You may only disclose this information in accordance with the requirements of the Privacy Act 1993, the Health Information Privacy Code 1994, section 22F of the Health Act, or any other statute or regulation permitting or requiring disclosure.

c) You must not share your HealthOne access code or password with anyone. You are responsible for any access that occurs under your password and logon details.

d) You understand that access will be monitored by the HealthOne Privacy Office and you agree to maintain a record of the purpose for viewing a patient's information in accordance with the procedure noted under Appendix 1.

e) You agree to co-operate fully with the HealthOne Privacy Office in relation to any investigation into access under this deed by the HealthOne Privacy Officer or any other lawful authority.

f) If you identify any unauthorised access to HealthOne or anything that may compromise the security of information in HealthOne, for example disclosure of your password, you will notify the HealthOne Privacy Office immediately.

g) If you no longer require access to HealthOne then you must notify the HealthOne Privacy Office immediately in writing. Upon notification the agreement is terminated.

4 HealthOne Rights:

a) HealthOne reserves the right to suspend your access to HealthOne at any time and for any reason, including for identified or suspected breaches of any aspect of this agreement. Where access is to be suspended you will be notified directly of the reason for the suspension and the likely duration of that suspension of access. Patient medical information can still be obtained by contacting the relevant health care provider such as a Community Provider, Pharmacist or DHB facility.

b) In the event of any inappropriate access the HealthOne Privacy Office may take further action including informing your employer or those working in association with you, informing the patient, or referring the matter to your professional registering authority.

c) HealthOne may amend the terms of the agreement or terminate the agreement for any reason by providing you with 30 days written notice.

5 Enforcement

a) HealthOne has the right to take action to enforce this agreement either jointly or severally.

6 Availability and Accuracy of Information:

a) While all reasonable efforts will be made to ensure that any health information made available is accurate, there is no warranty as to the accuracy, completeness or availability of the health information held on HealthOne. If you become aware of any inaccuracies in relation to the information then you must notify the HealthOne Privacy Office and the patient's treating clinician immediately.

7 Assignment, Delegation and Transfer:

a) Your access rights and related obligations under this agreement are personal to you, and shall not be assigned, sub-contracted, delegated or otherwise transferred.

8 Term:

a) This Access Deed remains in force until terminated in accordance with this agreement. Provisions intended to do so, for example access audit, will continue in full force and effect following termination.

I understand and agree to accept and abide by all the terms and conditions of this access deed.

I confirm the following:

1. **I acknowledge that this application is to gain access to the HealthOne applications and/or services and that my application is also subject to DHB approval**
2. **I consent to the information provided in this application being verified by my affiliated or registering healthcare authority**

ACCEPTED AND AGREED:

	First Name	***Other Names***	***Last Name***
Healthcare Professional Name:			
Email Address: (Required)			
Phone: *(Preferred Contact)*			
Signature:		***Date:***	

WITNESSED BY:

Name:			
Job Title:			
Signature:		***Date:***	

CONTACT DETAILS:

Practice Name:	
Practice Email:	
Address:	
Suburb:	
Phone:	

PROFESSIONAL ROLE:

Access Level	***Tick***	*Council*	***Number***
GP:		***NZMC:***	
RN:		***NCNZ:***	
Practice Staff:			
Pharmacist:		***CPN:***	
Pharmacy Technician:			
Allied Health *(Physio's and Therapists)*		***Discipline:***	

Security Information for HealthOne Access

If you need to call HealthOne Support, for example to reset your password, the information provided below will be used to authenticate you. This information is also used as part of the password self service system.

Full Name	
Personal Email Address	
Personal Mobile Phone Number	
Practice Name	
Job Title	

Authentication Questions

Please answer at least **two** of the questions below

First Pets Name	
First School	
Place of Birth	
Make or Model of First Car	
Memorable Person or Place	
Mother's Maiden Name	

Appendix 1 - Access and Audit Procedure

For Authorised Healthcare Provider Users Accessing HealthOne

Introduction

The HealthOne Access Deed for Healthcare Provider Users states:

"You understand that access will be monitored by the HealthOne Privacy Officer on behalf of DHB/HealthOne and you agree to maintain a record of the purpose for viewing a patient's information in accordance with the procedure noted under Appendix 1."

Privacy and Security

The Health Information Privacy Code requires the DHB take reasonable safeguards against inappropriate access and use of information. Each Healthcare Professional with access to HealthOne will sign an Access Deed which states they will only use HealthOne for its intended purpose, i.e., to support direct patient care. Healthcare Professional's are also bound by their professional code of ethics.

Audit of access is also an essential part of the HealthOne security structure. The HealthOne Privacy Officer will undertake a variety of audit procedures to ensure that access to healthcare information takes place for legitimate purposes only. You agree to cooperate with any request by the Privacy Officer for information regarding your reasons for accessing particular healthcare information for the purposes of audit activity. Any failure to cooperate with an audit request or to provide further information regarding reasons for access to a particular record or records may result in the immediate suspension or termination of our access agreement.

The audit procedures are based on establishing that you have in fact provided care to the patient and had legitimate reason to access their records. HealthOne must not be used to access own information or anyone else's information unless it is for the purpose of providing them with clinical care.

Reason for Access

The HealthOne Privacy Office will maintain a record of every access to a record by a healthcare provider. A *prima facie* justification for access is considered to be established where the records show that the Authorised User is part of a healthcare provider organisation which treats the patient or a dispensing record has occurred for that patient. This is known as Proximity Audit. Where this is not the case the Authorised User maybe required to provide a reason for accessing the patient's healthcare information.

This is the minimum level of record keeping which is enforced by HealthOne to determine the purpose for accessing a patient's healthcare information.

In addition, the HealthOne Privacy Officer may selectively undertake audits and may also proactively advise patients of who has accessed their records. This is known as Random Based Audit.

Requests for More Information

Patients may request from HealthOne detailed information on who has accessed their HealthOne healthcare information so that they can verify for themselves that all accesses have been appropriate. Typically this will involve the patient reviewing the log of who has accessed their records over time. Rather than looking at access to records from the perspective of health care providers the approach is focused on what activity has occurred. This is known as Patient Focused Audit.

If a patient questions the appropriateness of your access, you may be contacted by the DHB Privacy Office or the HealthOne Privacy Office to provide an explanation.

It is therefore recommended that you maintain further notes in your own System(s) on your purpose for accessing patient records in HealthOne, so that you can respond to any request for explanation. In this regard it should be noted that HealthOne Privacy Office reserves the right to undertake other audit activities as deemed appropriate for the purpose of ensuring the security and integrity of the HealthOne system and the privacy of patient healthcare information. You must co-operate with all such requests and provide any information requested by the DHB Privacy Office or HealthOne Privacy Office for audit purposes.

Inappropriate Access

Where any form of audit has failed to confirm the appropriateness of access, or the HealthOne Privacy Office has any reason to believe that access was not in accordance with the Access Deed, you will be informed and provided an opportunity to comment. If, after consideration of your response, the HealthOne Privacy Office still cannot confirm that the access was appropriate, The DHB Privacy Office or HealthOne Privacy Office may take further action including informing your employer or those working in association with you, informing the patient, or referring the matter to the Privacy Commissioner or to your professional registration authority.

Remote User Access

Access to HealthOne is via the DHB/Pegasus network. All access by HealthOne users outside the DHB/Pegasus network must be via a method approved by HealthOne and associated Information Systems teams.

Access to the DHB/Pegasus network must be done via a dedicated and secure remote access process (eg. Citrix or VPN). Direct dial-up into information systems or user PCs/computer workstations on the DHB/Pegasus network is prohibited.

A formal remote access registration, review and termination process shall be in place. All remote access requests must be approved by HealthOne Support.

Portable Computing

The use of portable, handheld or mobile devices (eg. notebooks, laptops, palmtops/PDAs, mobile phones) to access the DHB/Pegasus network systems must be managed.

All access to the device must be by the authorised user, and user identification and authentication must occur before the device is allowed to connect to the DHB/Pegasus network and information systems. This means credentials must not be saved on the device.

Confidential and sensitive information stored on portable devices must be protected from unauthorised viewing, eg. by use of encryption. This includes storage of information on devices such as portable memory keys.

Access to confidential and sensitive Healthcare information stored on portable computing devices must be secured via physical or logical power-on or log-on controls, Pin codes etc, where available.