St. Vincent's Hospital
390 Victoria St Darlinghurst 2010
Tel: (02) 8382 9100
Fax: (02) 8382 2188

SVHA Remote Access Application Form

- The use of this service is subject to Privacy and Confidentiality policy of the St Vincent's Health Australia Sydney and relevant State, Federal, and International criminal laws. This service is provided only for access to Web Clinical Applications and to provide support for SVHA applications.
- Under no circumstances are you permitted to use this service to conduct non-hospital related activities. Usage is monitored and abuse of this service will be reported.
- ITSC provides limited support for the use of this service on your personal computer and is not liable for any damages to your system configuration, software, or hardware.
- You are not to disclose remote access information to anyone else. This includes this document, access, login details, and passwords supplied.
- **ITSC now uses digital certificates as a security measure for remote access. This form must be accompanied by a photocopy of your driver's licence or passport details.**

Date Requested:	

Application Requested:	Netscaler/CTX ☐ Mediweb Result Viewer ☐ Powerpath Online ☐

***Title and Name**	
***Address**	
***Work Phone No**	
***Mobile Phone No**	
***Email Address**	
***Date of Birth**	**Day:** **Month :**

*** indicates mandatory information**
*** NB: DOB – Date of Birth (Not Year) is required as an additional unique identifier**

Remote Access Requirements

***Remote Access Connection Type**	**Tick Applicable**	***Operating Environment**	**Tick Applicable**
ADSL	☐	Windows 2000 / Windows XP	☐
Cable	☐	Macintosh OS 10	☐
Wireless	☐	Vista / Windows 7 or higher	☐

***My home PC or laptop has a current licence for anti-viral software with regular updates. If this requirement is not met – remote access will NOT be provided.	**Yes** ☐	**No** ☐

***Account User Declaration:** I acknowledge that I have read and understood the overview of the relevant Hospital Policies on Page 2 related to my responsibilities, in particular to the security of my LOGIN ID and PASSWORD and my obligations when using remote access. By signing this document, you have agreed to accept the above mentioned conditions. Please return a signed copy of this page + copy of identification by either return email or by faxing to 8382 2188. Your access password and instructions will be provided when the above information is received.

***Applicant's Signature**	**Date**

SVHA Sydney Terms and Conditions – Remote Access to SVHAS Network

Remote Access (Virtual Private Network VPN) Policy

The use of this service is subject to the Privacy and Confidentiality policy of the St Vincent's Health Australia, Sydney and relevant State, Federal, and International criminal laws. This service is restricted and provided only for access to Web Clinical Applications, to provide support for SVHAS applications and access to Outlook email.

Under no circumstances are staff permitted to use this service to conduct non-hospital related activities. Usage is monitored and abuse of this service will be reported. ITSC will provide manuals to assist staff to setup and maintain remote access and can provide limited support for the use of this service on user's personal computer. ITSC is not liable for any damages to their system configuration, software, or hardware due to remote access connection.

It is a mandatory requirement that staff have current antiviral software installed and are receiving regular Internet updates on personal PCs and laptops that are used to connect remotely to the SVHAS network. Staff are not to disclose remote access information to anyone else.

The SVHAS VPN has been implemented to meet the requirements of users roaming globally needing access to campus resources. This need is predicated by ease of use without the compromise of campus security. The VPN access needs to be easy and intuitive to use so that the roaming user is able to easily access campus resources from Internet Cafés and any external site (e.g. forums, hotels, airport lounges) with basic Internet access, or even from home (given an ADSL connection is available).

Confidentiality Policy

1. Information stored on the computer is only to be divulged to properly authorised persons. In the case of patient information, this is limited to treating health professionals and others authorised under the conditions detailed in Circular 99/18.
2. Staff must ensure that no unauthorised person has access to the SVHAS computing facility. This also means refraining from posting instructions for access onto or near the computer or anywhere a passerby or other unauthorised personnel may read them.
3. Staff will not under any circumstances divulge their username or password to any other person.
4. Staff must change the initial network login password that is allocated to them by ITSC.
5. Staff who use a group login will not divulge that information to any other person without the prior consent of their supervisor or department head, or in their absence, a senior member of the ITSC.
6. Wherever there is any question or doubt regarding to access to patient information, staff should refer to Circular 99/18. A copy is available on NSW Health Web site www.health.nsw.gov.au.
7. The attention of staff is drawn also to the contents of the document entitled SVHAS 'Code of Conduct' & Communication Policy available on the hospital intranet.

☐	**Driver's Licence**	☐	**Passport Details**
***Attach photocopy of your photo identification in the box below or attach to this form**			