DEPARTMENT OF HEALTH AND HUMAN SERVICES (DHHS)

INFORMATION TECHNOLOGY SERVICES (ITS)

<u>SEDI – SSL VPN REMOTE SERVICE END USER AGREEMENT</u>

January, 2009

<u>AGREEMENT</u>

Please read the following "**<u>DHHS, Information Technology Services (ITS), SEDI – SSL VPN Remote Service End User Agreement</u>**" carefully before using its services. By establishing a remote access account and using a Virtual Private Network (VPN), the user agrees to be bound by this Agreement and to use the Services in compliance with this Agreement.

<u>SERVICE REQUEST</u>

<u>Submittal</u>

Prior to receiving a remote connectivity account for the SEDI – SSL VPN service, each user must submit the following:

a) A signed "DHHS, Information Technology Services, SEDI – SSL VPN Remote Service End User Agreement" approved by the Primary Health Program Manager submitted to the DHHS – EDI Team at (Fax: 916-391-0762).
b) A signed "Information Technology Security Policy" agreement submitted to the DHHS – EDI Team at (Fax: 916-391-0762).

<u>Termination</u>

Should the SEDI - SSL VPN service become unnecessary, the Provider shall notify the DHHS EDI Team @ EDI-Dropbox@saccounty.net to have their SEDI - SSL VPN account deleted.

<u>USER REQUIREMENTS</u>

The user must have a privately purchased PC with the following requirements:

a) Operating System: Windows 2000, XP or Vista.
b) All software on the PC must be licensed and licensed agreements adhered to.
c) Must run and maintain a current version of anti-virus software.
d) Microsoft Internet Explorer 6.0 or later.

Additionally, the user will provide Internet connectivity.

USER RESPONSIBILITIES

Installation and Usage

a) Only authorized personnel may use the SSL VPN service to access the SEDI website/portal on the DHHS network.
b) The SEDI - SSL VPN service is for work-related activities only.
c) The user accepts full responsibility for installing and implementing the SEDI – SSL VPN service on their privately owned equipment.

Password Protection

a) Each individual is responsible for maintaining the security of IT resources including the security of their password.
b) When using the SEDI - SSL VPN service, the user's ISP subscriber name and ISP password shall adhere to a "Strong Password" convention.

- Be six to eight characters long.

- Contain at least one number between the first and last character.

- Contain at least one allowable symbol anywhere.

- Not contain more than two repetitious characters.

- Be significantly different from prior passwords.

- Not contain your user name or any part of your full name.

TECHNICAL SUPPORT

Privately Owned PCs

a) DHHS will provide installation and usage instructions for remote PCs.
b) DHHS will provide SEDI - SSL VPN Access Group logon IDs and passwords.
c) DHHS is not responsible for any problems encountered when using remote access software. Due to the diversity of hardware configurations, DHHS personnel are not familiar with the setup of the user's personal computer equipment. The County, the Department and ITS is not responsible for any problems that may occur or loss of functionality and/or data.
d) DHHS will not offer in-home support.
e) Please call the DHHS ITS Support Center to report any problems you may experience with your remote access. <u>Please verify that you have an active Internet connection before placing your call.</u> Regular work hours are 6:00 AM to 6:00 PM. 1-916-875-6123.

END USER ACKNOWLEDGMENTS

I have read and will abide by the conditions described in the above "**DHHS, Information Technology Services, SEDI - SSL VPN Remote Service End User Agreement**."

After providing your signature, email address and telephone number, please fax the signed **End User Acknowledgements** page to DHHS – EDI Team at (Fax: 916-391-0762). Please retain pages 1-3 for your reference.

_____   _____
User's Signature (required)   Date Signed (required)

_____
User's Printed Name (required)

_____   _____
User's Telephone Number (required)   Provider's Name (required)

_____   _____
User's Email Address (required)   Provider's County Vendor # (required)

PRIMARY HEALTH FISCAL ACKNOWLEDGMENTS

I authorize this remote access service request and certify that remote access is required for this individual. Additionally, I will ensure that prompt actions will be taken to notify the appropriate ITS personnel at such time as this account is no longer required.

_____   _____
Primary Health Fiscal Contact's Signature   Date Signed