1.0 Purpose:

To establish security standards for remote electronic Access to Texas Health Information Assets.

2.0 Policy:

Remote Access to Texas Health Information Assets should follow the requirements established in this policy to minimize security risks.

3.0 Scope:

This policy applies to:

3.1 Texas Health and its wholly owned or wholly controlled entities;

3.2 All Texas Health Workforce members, as well as members of Texas Health facility medical staff, trustees, contractors, and vendors.

3.3 Texas Health electronic Data and reports and Applications.

4.0 Definitions:

4.1 Access – the ability or means necessary to read, write, modify, or communicate Data/information or otherwise use any system resource.

4.2 Application Administrator – person that is responsible for administering the application, and maintenance activities which could include assigning access.

4.3 Automatic Updates – the process used where an application is configured (on a predetermined time basis) to connect to a server that contains the latest software, issues a request to the server to download the software and then installs the software locally with minimal manual intervention.

4.4 Broadband – a type of Data transmission in which a single medium (wire) can carry several channels at once (such as Digital Subscriber Lines (DSL), cable TV/modem, or two-way satellite).

4.5 Callback Modem – a modem that does not answer incoming calls. The modem requires the caller to enter a code and hang-up so the modem can call the

requestor back. If the entered code matches the previously authorized phone number, the modem dials the number.

4.6 Confidential – not made available or disclosed to unauthorized individuals, entities, or processes.

4.7 Data – any information in any medium including, but not limited to, desktop computers, laptop computers, telephones, fax machines, Personal Data Assistants (PDAs), and pagers, as well as variations, such as multi-function fax/printer/copiers, two-way pagers, PDA/phones, and paper.

4.8 Dial-Up Modem – a peripheral device that connects computers to each other for sending communications via the telephone lines. The modem modulates the digital Data of computers into analog signals to send over the telephone lines, then demodulates back into digital signals to be read by the computer on the other end.

4.9 Digital Subscriber Line (DSL) – a form of high-speed Internet Access that works over standard phone lines.

4.10 Dual-Homed – a Workstation with multiple network interfaces. A dual-homed Workstation can be used to create an unauthorized bridge between two separate networks. If one of the networks is compromised, the potential for the bridged network to be compromised increases significantly.

4.11 Health Information – any information, whether oral or recorded in any form or medium, that is created or received by a provider, plan, employer, or clearinghouse; and that relates to the past, present, or future health condition of an Individual, as well as the provision of healthcare to the Individual.

4.12 Individual – the subject of Health Information. This includes patients, Group Health Plan participants, and their covered dependents. Legally Authorized Representatives will be accorded the same rights regarding Uses and Disclosures of Health Information as the Individual.

4.13 Individually Identifiable Health Information – Health Information that identifies the Individual or provides a reasonable basis for doing so, by virtue of containing one or more of the eighteen identifiers specified by the Privacy Rule.

4.14 Integrated Services Digital Network (ISDN) – a set of standards for digital transmission of integrated analog or voice Data over ordinary telephone lines.

4.15 Legally Authorized Representative – (1) A parent or legal guardian, if the patient is a Minor; (2) a legal guardian, if the patient has been found by a court to be incapable of managing the patient's personal affairs; (3) an agent of the patient authorized under a medical power of attorney for the purpose of making a health care decision when the patient is incompetent; (4) an attorney ad litem and/or

guardian ad litem appointed for the patient by a court; (5) a personal representative or statutory beneficiary, if the patient is deceased, or heirs of the patient if no personal representative or statutory beneficiary exists; (6) an attorney retained by the patient or by the patient's legally authorized representative; (7) an attorney-in-fact of the patient. (See THR Policy on Health Information Uses and Disclosures for full definition).

4.16 Personal Firewall – a software application used to protect a single Internet connected computer from unauthorized users. The application or appliance device works in the background at the device (link layer) level to protect the integrity of the system from malicious computer code. This is accomplished by controlling Internet connections to and from a user's computer, filtering inbound and outbound traffic, and alerting the user to attempted intrusions.

4.17 Remote Access – the use of telecommunications to allow authorized Access to the Texas Health Network, Data, Reports and Applications.

4.18 Satellite – a specialized wireless transmitter/receiver placed in orbit around the earth that can allow Internet communications.

4.19 Split-Tunneling – a multiple branch networking path where some traffic is sent directly to the VPN server and other traffic is sent directly to the remote location without going through the VPN tunnel.

4.20 System Administrator – person that is responsible for administering the platform, including the operating system, and maintenance activities which could include assigning access.

4.21 Users – Texas Health Workforce members, members of Texas Health facility Medical Staff, Trustees/Directors, contractors, vendors, or others who use the Texas Health Electronic Communication Systems.

4.22 Virtual Private Network (VPN) – a way to securely communicate over the Internet to a corporate network through a dedicated server that uses encryption or other secure mechanisms.

4.23 Workforce – employees, volunteers, persons involved in Texas Health training programs or those sponsored by its wholly owned or wholly controlled entities, and other persons whose conduct, in the performance of work for an entity, is under the direct control of such entity, whether or not they are paid by the entity.

4.24 Workstation – information processing equipment, including microcomputers, Personal Digital Assistants, laptops, and wireless devices.

5.0 General Requirements:

5.1 Authorized Workforce members should only use Innovative Technology Solutions (ITS) approved Remote Access Technology.

5.2 Remote Access should be secured, controlled, and granted on a need to Access basis.

5.2.1 Examples of Remote Access technologies are:

a. Integrated Services Digital Network (ISDN)

b. Digital Subscribers Lines (DSL)

c. Cable and Dial-Up Modem

d. Virtual Private Network (VPN)

5.2.2 Examples of Remote Access applications are:

a. Citrix

b. Terminal Services

c. Virtual Private Network (VPN)

5.3 When Remotely connecting to Texas Health's network using the Citrix application, the equipment used must have, at a minimum, the following installed:

5.3.1 virus management software configured for automated updates to help prevent introducing virus or malicious code into the Texas Health network;

5.3.2 the workstation must be configured for automatic operating system updates to help minimize system or application vulnerabilities from being exploited.

5.4 When remotely connecting to Texas Health's network through other approved ITS technologies that does not include the Citrix application, the equipment used must have, at a minimum, the following installed:

5.4.1 a personal firewall application or appliance device that actively manages Internet connectivity to help prevent unauthorized Access to Texas Health assets; A list of Texas Health recommended applications and devices will be listed on the Texas Health information security website.

5.4.2 virus management software configured for automatic updates to help prevent introducing virus or malicious code into the Texas Health network;

5.4.3 the workstation must be configured for automatic operating system updates to help minimize system or application vulnerabilities from being exploited.

5.5 The use of Split-tunneling or Dual Homing to Access the Texas Health network must be pre-approved by ITS.

5.6 Routers for dedicated ISDN lines configured for Access to the Texas Health network should meet the minimum encryption standards according to the Encryption Policy.

6.0 Users:

The Remote Access connection between the person's location and Texas Health are extensions of Texas Health's network and provide a potential path to PHI or Confidential information. Texas Health Workforce members should use reasonable security measures to protect Texas Health's assets.

6.1 Reasonable security safeguards should be implemented on a person's personal equipment used to connect to the Texas Health network.

6.2 Remote Access to the Texas Health network should be used for work related purposes only.

6.3 Texas Health PHI, Confidential Information, or applications should not be stored to the hard drive of the Remote Access computer or any other non-Texas Health storage media.

6.4 Remote session to the Texas Health network should be terminated by selecting the logoff option. If only the Remote Access session browser is closed, the remote session is still active and can potentially be used by non-authorized Workforce or Vendors.

7.0 Dial-ups, Modems, Internet Service Providers:

7.1 Texas Health Computers accepting remote connections should:

7.1.1 Authenticate each User, at a minimum, by a unique identification with a password and should encrypt the Data stream;

7.1.2 Include a time-out to terminate inactive sessions;

7.1.3 Temporarily terminate the connection or time-out the User ID following a sequence of five to seven unsuccessful attempts to login.

7.2 Modems installed on Texas Health computers or servers for Remote Access must be pre-approved by ITS.

8.0 Administrative Access:

8.1 Application or System Administrators Access should be through Citrix or other approved Remote Access servers and not by directly dialing into a modem connected to a computer to provide remote support. This opens a vulnerable network link and creates a security risk.

8.2 Access protocols vulnerable to exploitation (e.g., telnet, ftp) should not be used unless transmission is through an encrypted tunnel such as a VPN.

8.3 Remote control Access (e.g., PCAnywhere) should be configured according to ITS security standards and at a minimum should:

8.3.1 Deny dial-up connectivity unless transmissions are encrypted;

8.3.2 Use Callback Modems programmed to call authorized User numbers to verify the request is from an authorized number; or

8.3.3 Use IP address screening for Broadband connections.

9.0 Vendor Maintenance and Technical Support:

9.1 Certain vendors will be granted limited Remote Access to the Texas Health network to provide routine maintenance and technical support (excluding support provided during the initial installation of an application or computer system).

9.2 The Workforce member responsible for the vendor relationship follow the IS Remote Account Administration Procedures when requesting vendor access.

9.3 Certain Texas Health Information Assets are configured to automatically contact a vendor to report a technical problem when the application or system generates an alert.

9.3.1 This type of automatic response must be pre-approved by ITS and the application or system administrator. After approval, the vendor will be granted a login ID and password to provide support for the length of the contracted services.

9.3.2 The vendor is responsible for notifying Texas Health about all support activities within 24 hours or according to the established service agreement.

10.0 Policy Violations And Sanctions:

Violations of this policy will be processed according to applicable Texas Health policies, including the Progressive Corrective Action Policy, as well as civil and criminal laws.

11.0 Other Applicable Policies:

11.1 Encryption

11.2 Computer Virus Management

11.3 Confidentiality

11.4 Data Access Control

11.5 HR Information Privacy and Security Inquiries Complaints and Breaches

11.6 Information Privacy and Security Sanctions

11.7 Password Management

11.8 Safeguarding Health Information

11.9 Telecommuting

11.10 Progressive Corrective Action

11.11 Workforce Security