

HQ IT Standard: VPN Policy	
SIGNATURE: <i>Robert Gilliland</i>	DATE ISSUED: 7-24-09 DATE REVIEWED: 3-27-16
APPROVED: Robert Gilliland	VERSION: 2.0
REFERENCE NUMBER: HQ.8.5.14	PAGE: Page 1 of 2

1.0 PURPOSE

The purpose of this policy is to provide guidelines for Remote Access IPsec or SSL Virtual Private Network (VPN) connections to the Health Quest corporate network.

2.0 SCOPE

This policy applies to all Health Quest employees and its affiliates, contractors, consultants, temporaries, and other workers including all personnel affiliated with third parties utilizing VPNs to access the Health Quest's network. This policy applies to implementations of VPN that are directed through an IPsec or SSL Concentrator.

3.0 POLICY

Approved Health Quest employees and authorized third parties (customers, vendors, etc.) may utilize the benefits of VPNs, which are a "user managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees

Additionally,

1. It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to Health Quest internal networks.
2. VPN use is to be controlled by having the user fill out a request to access VPN, be put in appropriate group and given an Active Directory account.
3. All HQ destined traffic will be encrypted between client and VPN using approved encryption policies.
4. VPN gateways will be set up and managed by Health Quests network support groups.
5. All computers connected to Health Quest internal networks via VPN or any other technology must use the most up-to-date anti-virus software that is the corporate standard.
6. VPN users will be automatically disconnected from Health Quest's network after thirty minutes of inactivity. The user must then logon again to reconnect to the network
7. Users of computers that are not Health Quest owned equipment must configure the equipment to comply with Health Quest's VPN and Network policies.
8. Only Citrix Access Gateway clients are approved VPN clients that may be used.

Revision #:	2.0	Supersedes:	Version 1.0	Date:	08/24/10
--------------------	-----	--------------------	-------------	--------------	----------

HQ IT Standard: VPN Policy	
SIGNATURE: <i>Robert Gilliland</i>	DATE ISSUED: 7-24-09 DATE REVIEWED: 3-27-16
APPROVED: Robert Gilliland	VERSION: 2.0
REFERENCE NUMBER: HQ.8.5.14	PAGE: Page 2 of 2

9. By using VPN technology with personal equipment, users must understand that their machines are a de facto extension Health Quest's network, and as such are subject to the same rules and regulations that apply to Health Quest owned equipment.

4.0 REVISION HISTORY

Date	Revision #	Description of Change
07/24/09	1.0	Initial creation.
08/24/10	2.0	Added Citrix VPN to policy
03/27/16	3.0	Removed Cisco VPN client access

5.0 INQUIRIES

Direct inquiries about this policy to:

Robert Diamond, CIO
 21 Fox St
 Poughkeepsie, NY 12601
 Voice: 845-483-6701
 Fax: 845-483-6776
 E-mail: rdiamond@health-quest.org

Revision #:	2.0	Supersedes:	Version 1.0	Date:	08/24/10
--------------------	-----	--------------------	-------------	--------------	----------