I. PURPOSE
To define requirements for connecting to Denver Health’s (DH) network from any remote host. These requirements are designed to safeguard DH from damages that may result from unauthorized use of DH resources.

II. POLICY
It is the policy of DH to protect its network and internet connections from unauthorized use. Access to DH’s network and internet connections, and the information therein, is protected under the Health Information Technology for Economic and Clinical Health Act (HITECH Act) and the Health Insurance Portability and Accountability Act (HIPAA).

III. DEFINITIONS
A. Remote Access: All forms of web-based, client-based and point-to-point remote access methods used to do work on behalf of DH, including but not limited to reading or sending e-mail and viewing intranet resources.

B. Virtual Private Network (VPN): A communications network tunneled through another network, and dedicated for a specific network. A third party will be granted VPN access only after entering into a Memorandum of Understanding with DH.

IV. RESPONSIBILITY
A. eHealth Services (eHS), Rocky Mountain Poison & Drug Center, BioMed, and other technology managers ensure compliance with security measures on all computing and network resources they are responsible for.

B. All DH managers and supervisors are responsible for ensuring unauthorized users are not allowed access to DH internal networks.

V. METHODOLOGY
A. This policy applies to all DH employees, contractors, temporary employees, vendors and agents and includes DH owned and non-owned computers, workstations, laptops or other mobile devices used to connect to DH computing and networks resources.
B. Network Protection:
1. Secure remote access is strictly controlled. The eHS Security Department selects the style of connection appropriate for the user-based requirements.
2. Control is enforced using a DH issued user ID and password, two-factor authentication, or public/private keys with strong password phrases.
3. DH login or password information should be treated as confidential and not shared with anyone (i.e., family members, DH Help Desk, or co-workers).
4. VPN users are automatically disconnected from DH’s network after thirty minutes of inactivity.
   a. Users must log back in to reconnect to the network.
   b. Use of pings or other artificial network processes to keep the connection open are prohibited.
5. If non-DH-owned equipment is used, configure the equipment to comply with DH policy.
6. Do not connect computers or workstations, which are remotely connected to DH’s corporate network, to any other network at the same time; with the exception of personal networks that are under the complete control of the user.
   a. Split (dual) tunneling is not allowed. When actively connected to the DH network, VPN clients will force all traffic to and from the PC over the VPN tunnel; all other traffic is dropped. If split (dual) tunneling is enabled the connection will be dropped.
   b. Reconfiguration of a user’s equipment for the purpose of split-tunneling is not permitted at any time and may result in the connection to DH being dropped.

C. Remote access:
1. Remote access implementations include, but are not limited to: DSL (e.g., Century Link DSL), cable modems (e.g., Comcast) and VPN.
2. All remote access to DH networks must be encrypted in a method approved by eHS Security and eHS Network.
3. Unencrypted/unsecured remote access to DH’s network is prohibited.
4. It is the responsibility of all employees and contractors with remote access privileges to DH’s network to ensure their remote access connection is given the same attention and careful consideration as their on-site connection.

D. General:
1. Unauthorized use of DH networks or internet connection by anyone other than authorized DH employees or contractors while connected via remote access is prohibited.
2. Patient data, sensitive or confidential data must be viewed privately preventing unauthorized users access to the information.
3. Printing of protected health information (PHI), sensitive or confidential data is strictly prohibited.
   a. Prior written approval from the department of Health Information Management (HIM) must be received before printing.
   b. Ensure there is access to a properly contained shredding device.
E. Practical Implications:
1. Use of non-DH email accounts (e.g., Hotmail, Yahoo, AOL or Gmail) or other external resources is prohibited when conducting DH business, thereby ensuring official business is never confused with personal business.
2. Only eHS Network and eHS Security approved VPN clients may be used.
3. Organizations or individuals who wish to implement non-standard remote access solutions to DH’s network must obtain prior approval from eHS Security, eHS Networking and the Chief Technology Officer (CTO) via standard eHS processes (eMAC or project request).
4. Third party vendor connections must comply with requirements as stated in the Third Party Agreement.
5. By using a VPN client on personal equipment, users understand that their computers are a de facto extension of the DH network. As such, they are subject to the same rules and regulations that apply to DH-owned equipment; computers must be configured in a manner that complies with DH, eHS Security and eHS Network policies.

F. Personal equipment used to connect to DH’s networks:
1. Use the most up-to-date anti-virus software and virus signatures, as well as current operating system patches. Connections to the DH network may be delayed, denied, or terminated without these items.
2. User’s home network must use industry standard and DH approved security authentication/encryption for WiFi.
3. Pre-shared keys and passwords on home networks must meet DH password policy and encryption standards.

G. Policy Violation:
1. Circumvention of security controls for computing and network resources.
2. Assisting or requesting anyone to circumvent security.
3. Violations of this policy may result in disciplinary action, up to and including termination.

VI. REFERENCES
A. Denver Health Policies & Procedures:
1. P-6.019 Electronic Messaging
2. P-6.021 User Account Password
3. P-6.024 Mobile Computing Devices
4. P-6.027 Computing and Network Security Policy
5. P-6.026 Information Systems User Access

B. Denver Health Human Resources Employee Principles & Practices:
1. #4-146 Enforcement & Discipline Regarding Inappropriate Health Record Accesses
2. #4-129, Employee Counseling and Corrective Action

C. Denver Health eHS Procedures:
1. DG-6.01, Wireless Device Risk Assessment
DENVER HEALTH

POLICY

2. DP-6.90, Denver Health Wireless Network Standards
3. DPR-6.65 How to Request VPN Access


   1. 45 CFR Part 160 and Part 164, Subparts A and C.
   2. Health Information Technology for Economic and Clinical Health Act (HITECH Act), Subtitle D; enacted as part of the American Recovery and Reinvestment Act of 2009Denver.

VII. APPENDICES
    DH Acknowledgement Page.
ACKNOWLEDGEMENT

By signing below, I affirm that I have read, understand, and agree to fulfill the provisions of the Remote Access and Virtual Private Network (VPN) Policy.

______________________________
Printed Name

______________________________
Signature

______________________________
Date