Origination:	*07/2010*
Effective:	*01/2018*
Last Approved:	*01/2018*
Last Revised:	*01/2018*
Next Review:	*01/2021*
Owner:	*Iain Lumsden: IS Security Manager*
Document Area:	*Information Technology/ eHS*
Document Type:	*Policy*
Applicability:	*Denver Health*

Remote Access and Virtual Private Network (VPN)

PURPOSE

The purpose of this policy is to define rules and requirements for connecting to the Denver Health and Hospital Authority (DHHA) network from any remote host. These rules and requirements are designed to safeguard DHHA from damages that may result from unauthorized use of DHHA resources. Damages include loss of confidential or sensitive data, such as protected health information (PHI), damage to public image, damage to critical DHHA internal systems, and fines, or other financial liabilities incurred as a result of those losses.

The following sections are included in this policy:

[Requests and Approvals for Remote Access and VPN](#)
[Network Control and Protection](#)
[Remote Access](#)
[General Guidelines on Use](#)
[Practical Implications](#)
[Personal Equipment Used to Connect to DHHA's Networks](#)

SCOPE

This policy applies to Denver Health and Hospital Authority (DHHA) – All departments including DHHA employees, contractors, consultants, temporary employees, vendors, and any other agents connecting to DHHA networks from a remote host. This policy is applicable to all equipment and systems used for remote access including DHHA-owned and personal (employee-owned) computers, desktops, laptops, and any other type of workstation, or other mobile computing devices used to connect to DHHA computing and network resources. This policy does not cover requirements for accessing DHHA's Guest Wireless Network or securing the servers and applications that are remotely accessed.

INCLUSIONS/EXCLUSIONS

A. DHHA employees, contractors, consultants, temporary employees, vendors, and any other agents connecting to DHHA networks from a remote host *shall* adhere to this policy and refrain from any activity that might circumvent this policy. DHHA employees and other individuals working on behalf of DHHA *shall not*:

   1. Circumvent any security controls for computing and network resources.
   2. Assist or request anyone to circumvent security.

B. System administrators shall ensure technical controls and operational procedures are in place to identify, prevent, correct, and report violations of this policy.

C. All DHHA managers and supervisors are responsible for ensuring only authorized users are approved to access DHHA internal networks.

D. eHealth Services (eHS) managers and supervisors are responsible to ensure compliance with this policy and security measures on all computing and network resources they are responsible for.

E. Failure to comply with the requirements and restrictions defined in this policy can result in corrective action up to, and including termination.

DEFINITIONS

Duo Mobile: Duo Mobile works with Duo Security's two-factor authentication service to make network logins more secure. The application generates passcodes for login (user ID account and password) and can receive push notifications for one-tap authentication. Additionally, Duo Mobile is used to manage two-factor authentication for other applications and web services that make use of passcodes. Note: Duo Mobile needs to be activated and linked to your user ID account before it will work.

Mobile computing device: Includes laptop computers, iPads, tablets, smartphones, Windows Mobile devices, Android-based devices, and any mobile device capable of storing DHHA data and connecting to an unmanaged network.

Protected health information (PHI): Individually identifiable health information that the health care components of the covered entity created, received, maintained, or transmitted in any form or medium. All references to "PHI" or "electronic PHI" refer to PHI.

Remote access: The ability to log onto a network from a distant location, which allows employees to work off-site. Remote access is set up at DHHA using a Virtual Private Network (VPN), so that systems and networks can be accessed remotely. This includes all forms of web-based, client-based, and point-to-point remote access methods used to do work on behalf of DHHA, including but not limited to reading or sending email and viewing intranet

resources.

Service Request: Cherwell Service Management™ tool used to request IT services and support via the eHealth Services Portal (or via the Help icon on the desktop). A Service Request is used to order new equipment, system access, application installation, and/or other Information Technology (IT) deliverables.

Split tunneling: The process of allowing a remote VPN user to access a public network, most commonly the Internet, at the same time that the user is allowed to access resources on the VPN.

Two-factor authentication (TFA): TFA, also known as 2FA, is an extra layer of computing access security control. It is a method of confirming a user's claimed identity by utilizing a combination of two different components. It requires not only a username and password, but also something only that user has on them (i.e., a piece of information only they should know or have immediately on hand such as a physical token).

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 DHHA. Site-to-site VPN connections are used between DHHA and vendors, as needed.

POLICY

It is the policy of DHHA to protect its network and Internet connections from unauthorized use. Access to DHHA's network and Internet connections, and the information therein, is protected under the Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health (HITECH) Act. All remote access users must follow the mandatory minimum standards in this policy.

PROCEDURES

A. Requests and Approvals for Remote Access and VPN

1. Obtain your supervisor's approval for remote access and VPN privileges.
2. Requests are entered and authorized via the eHealth Services Portal (or via the Help icon on the desktop), Service Request process.
    a. In the portal, select **Request**.
    b. On the Catalog of Services web page, select **Security**.
    c. Fill in the New Service Request form.
        i. Make sure to select the **VPN – Remote Access** checkbox.
        ii. If you are requesting site-to-site VPN access for a vendor or contractor, make sure to include this information in the Business Justification/Additional Details text box.
        iii. Attach documents or forms, as needed.
    d. Save the form.
3. Approval is required from the requester's Executive Staff or designee and from the eHS IS Security Manager.
4. If the request involves multiple departments, it is considered a Project Request; therefore, submit the eHS Project Request Form with your Service Request. Note: This form is available in the Denver Health Pulse, Administrative Services, eForms, under PC/Technology).
5. The requester will be contacted by an eHS Security analyst or technician.
6. Read this policy and sign the Acknowledgment Signature Page (Attachment A).

To top

B. Network Control and Protection

1. Secure remote access is strictly controlled. The eHS IS Security team selects the style of connection appropriate for and based on user requirements in the Service or Project Request.
2. Control is enforced using a DHHA-issued user ID account and password (login information), two-factor authentication, or public or private encryption keys with strong password phrases.
3. DHHA user ID account (username) and password information should be treated as confidential and not shared with anyone, such as family members, coworkers, including Help Desk personnel. For more details, refer to User Account Password, Information Systems User Access, and Computing and Network Security policies.
4. VPN users are automatically disconnected from DHHA's network after 30 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. Only one network connection is allowed.
    a. Do not connect computers, workstations, laptops, or other mobile computing devices which are remotely connected to DHHA's network to any other network at the same time; except personal networks that are under the complete control of the user. For more information, refer to the Personal Equipment Used to Connect to DHHA's Networks section below.
    b. Split (dual) tunneling is *not permitted*.
        i. If split tunneling is enabled, the connection to DHHA will be dropped.

ii. When actively connected to the DHHA network, VPN clients will force all traffic to and from the personal computer over the VPN tunnel; all other traffic is dropped.

6. If personal equipment is used to connect to the DHHA network, configure the equipment to comply with DHHA policy. For more information, refer to the Personal Equipment Used to Connect to DHHA's Networks section below.

C. Remote Access

1. Remote access implementations include, but are not limited to: wireless networks, Digital Subscriber Line (DSL), cable modems, and VPN.
2. All remote access to DHHA networks must be encrypted in a method approved by the eHS IS Security team and eHS Network and Telecommunications team.
3. Unencrypted and unsecured remote access to DHHA's network is prohibited.
4. Duo Mobile Security's two-factor authentication is required for remote access to the DHHA's network. Note: This added precaution is to ensure remote access to Clinical Desktop or Remote Desktop via VPN (Citrix Receiver or Cisco AnyConnect) is more secure.
5. It is the responsibility of all DHHA employees, contractors, consultants, temporary employees, vendors, and any other agents connecting to DHHA networks from a remote host with remote access privileges to DHHA's network to ensure their remote access connection is given the same attention and careful consideration as their on-site connection.

To top

D. General Guidelines on Use

1. Unauthorized use of DHHA networks or Internet connections by anyone other than authorized DHHA employees, contractors, consultants, temporary employees, vendors, or other individuals while connected via remote access is prohibited. For more information, refer to Information Systems User Access Policy.
2. PHI, sensitive, or confidential data must be viewed privately to prevent unauthorized users access to the information. For more information, refer to Monitoring Unauthorized Access to Protected Health Information.
3. Printing of PHI, sensitive, or confidential data is strictly prohibited. Prior to printing, ensure the following:
   a. Prior written approval from the eHS Health Information Management (HIM) department is received.
   b. Access is available to a properly contained shredding device.

E. Practical Implications

1. Use of non-DHHA email accounts (e.g., Gmail, Hotmail, Yahoo, AOL, etc.) or other external resources is prohibited when conducting DHHA business. This is to ensure official DHHA business is never confused with personal business. For more information on email use policies, standards, and requirements, refer to Mobile Computing Devices Policy, and Electronic Messaging - Email, Texting, Mobile Photography Policy.
2. Only the eHS IS Security team and eHS Network and Telecommunications team approved VPN clients will be used.
3. Organizations, departments, or individuals who wish to implement non-standard remote access solutions to DHHA's network must obtain prior approval from the eHS IS Security manager, eHS Network and Telecommunications manager, and the Chief Technology Officer (CTO) or Senior Director of IT Operations via standard eHS processes such as the Service Request or Project Request, as required.
4. Third-party vendor connections must comply with requirements as stated in the third-party agreement with DHHA. For more information on vendor and contract agreement requirements, refer to Contract Policy.
5. By using a VPN client on personal equipment, users understand that their computers, laptops, and/or other mobile computing devices are a *de facto* extension of the DHHA network. As such, they are subject to the same rules and regulations that apply to DHHA-owned equipment, and must be configured in a manner that complies with DHHA, eHS Security, and eHS Network policies. For more information, refer to the Personal Equipment Used to Connect to DHHA's Networks section below and Computing and Network Security Policy, Information Security Incident Management policy, Mobile Computing Devices Policy, and Wireless Network Policy.

F. Personal Equipment Used to Connect to DHHA's Networks

1. Use the most up-to-date antivirus software and virus signatures, as well as current operating system patches. Note: Connections to the DHHA network may be delayed, denied, or terminated without these items.
2. The user's home network must use industry standard and DHHA-approved security authentication and encryption for wireless networks, cable, or DSL connections.
3. Pre-shared encryption keys and passwords on home networks must meet DHHA password policy and encryption standards.
4. For more details on DHHA password, network, and personal equipment use policies, standards, and requirements, refer to User Account Password Policy, Computing and Network Security Policy, Mobile Computing Devices Policy, and Wireless Network Policy.

To top

DOCUMENTATION/RECORDS

A. Additional Security Requirements for Remoting into the Denver Health Network (also known as Mobile Security Job Aid)

B. eHealth Services Portal (Denver Health Pulse, Useful Links)

C. eHS Project Request Form (Denver Health Pulse, Administrative Services, eForms, PC/Technology)

D. How to Connect to the Denver Health Network Remotely: User instructions for Accessing the Clinical Desktop and Other Published Citrix

Applications Remotely (Cherwell Knowledge Article No. 31810)

E. Remote Access/Citrix Receiver Changes tip sheet (August 2017) (Denver Health Pulse, eHealth Services, 2013 Site Directory, Project Management Office, IT Quality Office, Instructional Design & Training Team, Job Aids and Tip Sheets, Citrix)

F. User Troubleshooting Duo Mobile for Remoting into the Denver Health Network (also known as Duo Mobile Job Aid)

EXTERNAL REFERENCES

A. Health Insurance Portability and Accountability Act (HIPAA) of 1996. 45 *CFR* Part 160 and Part 164, Subparts A and C. Public Law 104-191. August 21, 1996. Available at http://www.gpo.gov/fdsys/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf

B. Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII—Health Information Technology, Subtitle D—Privacy, enacted as part of the American Recovery and Reinvestment Act of 2009. Available at https://www.gpo.gov/fdsys/pkg/PLAW-111publ5/pdf/PLAW-111publ5.pdf

C. HITECH Breach Notification Interim Final Rule. 45 *CFR* Parts 160 and 164; August 19, 2009. Available at https://www.gpo.gov/fdsys/pkg/FR-2009-08-24/pdf/E9-20169.pdf

D. Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules. 45 *CFR* Parts 160 and 164; January 25, 2013. Available at http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf

E. Payment Card Industry Data Security Standards (PCI-DSS), version 2.0, October 2010. Available at https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf

F. Standards for Privacy of Individually Identifiable Health Information; Final Rule. 45 *CFR* Parts 160 and 164; August 14, 2002.

DHHA RELATED DOCUMENTS

A. Contract Policy

B. Computing and Network Security Policy

C. Disciplinary Action for Violations of HIPAA Privacy and Security Policies

D. Electronic Messaging – Email, Texting, Mobile Photography

E. Employee Counseling/Accountability Based Performance

F. Information Security Incident Management

G. Information Systems User Access

H. Mobile Computing Devices

I. Teleworking

J. User Account Password

K. Wireless Network Policy

ATTACHMENTS

Attachment A – Acknowledgment Signature Page (January 2018)
Attachment B – How to Connect to the Denver Health Network Remotely: User Instructions for Accessing the Clinical Desktop and Other Published Citrix Applications Remotely (October 2016)

Attachments:

Attachment A – Acknowledgment Signature Page
Attachment B – How to Connect to the Denver Health Network Remotely: User Instructions for Accessing the Clinical Desktop and Other Published Citrix Applications Remotely

Approval Signatures

Step Description	Approver	Date
	Robin Wittenstein: Chief Executive Officer	01/2018
	Joe Jaudon: Chief Technology Officer	01/2018
	Nancy Holtzmaster: Applications Management Mgr.	12/2017
	Randall Frietzsche: Chief Information Security Officer	12/2017
	Bryan Leary: IT Director Applications [CM]	12/2017
	Jeffrey Pelot: Chief Information Officer	12/2017
	Tony (John) Fournier: Business Continuity & Disaster Recovery Manager	11/2017
	Iain Lumsden: IS Security Manager	11/2017

Step Description	Approver	Date
	Kim Nelson: Sr Director IT Operations	11/2017
	Diane Verrilli: Sr Technical Writer (IT)	11/2017
Formatting Review	Colette Morris: Program Manager of Document Management	11/2017
	Iain Lumsden: IS Security Manager	11/2017