

UNC School of Medicine Remote Access Policy

Purpose

The purpose of this policy is to define standards for connecting to the UNC School of Medicine's network resources from any host located outside of the School of Medicine's physical or logical network. These standards are designed to minimize the potential for unauthorized use of School of Medicine resources. Such unauthorized use could result in the loss or compromise of sensitive or confidential data, intellectual property, and critical School of Medicine internal systems.

Scope

This policy applies to all School of Medicine faculty, staff, students, contractors, vendors and agents with a School of Medicine-owned or personally-owned computer or workstation used to connect to the School of Medicine network. This policy applies to all connections to devices on the School of Medicine network (including servers and desktop computers) originating from devices outside of the School of Medicine network.

Policy

General

1. It is the responsibility of School of Medicine faculty, staff, students, contractors, vendors and agents with remote access privileges to the School of Medicine's network to ensure that their remote access connection complies with the same security requirements as the user's on-site connection to the School of Medicine. Solutions for remote access to devices on the SOM network must comply with established University of North Carolina at Chapel Hill, School of Medicine and UNC Health Care System policies where applicable, specifically:
 - a. *UNC Health Care Information Security Policy*
<http://www.med.unc.edu/security/hipaa/documents/Information%20Security%2012-18-07.pdf>
 - b. *School of Medicine Password Policy*
http://www.med.unc.edu/security/hipaa/documents/password_policy_09-15-05.pdf
 - c. *School of Medicine Desktop Configuration Policy*
http://www.med.unc.edu/security/hipaa/documents/Desktop_Configuration_Policy_2009.pdf
 - d. *UNC Acceptable Use Policy*
<https://help.unc.edu/1672>
 - e. *School of Medicine Network Access Security Policy*
http://www.med.unc.edu/security/hipaa/documents/Network_Access_and_Security_Policy_Final.pdf

Requirements

1. Secure remote access must be strictly controlled through strong authentication in accordance with the School of Medicine Password Policy.
2. At no time should any user of School of Medicine network resources provide their login or email password to anyone, not even family members. When using a shared personal computer, for example, users should employ encryption and setup separate accounts so that other users of the computer can not access sensitive data.
3. Connections used to transfer protected health information (PHI) and confidential or internal information, as defined by the School of Medicine Information Security policy, must encrypt all traffic between the remote client and server with solutions that fall into generally accepted best practices such as the use of a VPN or SSL. Additionally, any files containing PHI or other confidential information transferred to and stored on a personal computer must be stored in a way that prevents other users of the computer from accessing the data without authorization.

4. If connecting through a router that has a wireless transmitter, whether connected through either the wired or wireless ports, the transmitter must be configured in an encrypted mode or it must be turned off.
5. All hosts, including personal computers, which are connected to the School of Medicine internal networks via remote access technologies must be using active anti-virus software when possible, including the most current virus definitions. All connecting hosts must also be updated with the latest security patches for the operating system of the connecting host.
6. Personal devices that are used to connect to the School of Medicine's network must meet the same requirements of University owned devices.
7. Remote access connections directly to office workstations on the School of Medicine network using applications such as Windows Remote Desktop, PC Anywhere, Go To My PC, VNC, SSH, etc. are acceptable, provided that:
 - a. the software is approved by the School of Medicine Information Security Officer;
 - b. the software must use encryption from end to end;
 - c. the workstation on the School of Medicine network MUST be configured with authentication rules meeting the requirements of the School of Medicine Password Policy;
 - d. the workstation on the School of Medicine network must be configured so that authentication is required for use and only authorized users are allowed access; and
 - e. the remote computer making the connection must meet the minimum requirements of the School of Medicine Workstation Security Policy.
8. Users must ensure proper physical security precautions are taken when connecting to the School of Medicine network from remote locations. For example:
 - a. Machines must not be left unattended while connected or logged into the School of Medicine network.
 - b. In public environments, users must take precautions to prevent unwanted viewing of computer screens by unauthorized persons.

Enforcement

Any person found to have violated this policy may be subject to permanent suspension of access to School of Medicine network resources. Employees may be subject to disciplinary action, up to and including dismissal.

Definitions

Confidential Information

See the UNC Health Care Information Security Policy, Section VI - Information Classification.

The policy is available at

<http://www.med.unc.edu/security/hipaa/documents/Information%20Security%202012-18-07.pdf>

Protected Health Information (PHI)

See the UNC Health Care Information Security Policy, Section VI - Information Classification.

The policy is available at

<http://www.med.unc.edu/security/hipaa/documents/Information%20Security%202012-18-07.pdf>

Remote Access

Remote Access is any access to the School of Medicine's corporate network through a network, device, or medium not controlled by the School of Medicine.

SSH

Secure Shell is a cryptographically strong replacement for login, telnet, ftp, and other programs that protects against "spoofing," man in the middle attacks, and packet sniffing.

SSL

Secured Sockets Layer is a protocol that transmits communications over the Internet in an encrypted form. SSL ensures that the information is sent, unchanged, only to the intended server. Online shopping sites frequently use SSL technology to safeguard your credit card information.

VPN

Virtual Private Network is a way to communicate through a dedicated server securely to a corporate network over the internet.

Approved by the HIPAA Planning and Oversight Council (HPOC): March 22, 2005

Revised February 2009

Approved by the HIPAA Planning and Oversight Council (HPOC): March 5, 2009