UNM Health System Virtual Private Network (VPN) Access Authorization for Remote Network Access

I understand that signing this form allows me to access the University of New Mexico Health Sciences Center (UNM HSC) internal network remotely through my UNM Hospitals (UNMH) or HSC account. I understand that UNM HSC must control remote access to its internal computing systems to ensure that electronic protected health information (ePHI) and other sensitive data are accessed only from secure workstations. I will employ appropriate safeguards and practices while accessing HSC computing systems. I understand that VPN access is provided as a mechanism for access to HSC systems when alternative access methods are insufficient.

- I agree to protect patient and employee confidential data and to never disclose my password to anyone or allow my password to be stored in any manner.
- I agree to protect my screen from unauthorized viewing and not access clinical or sensitive systems in public areas.
- I will log out of the HSC system at the end of my session and disconnect from the VPN or lock my session if I leave my computer unattended.
- I agree that I will never access ePHI from an untrusted computer.
- I agree that the workstation I use will have the most recent security patches installed and have up-to-date antiviral software running.
- If the computer I am using has been compromised, I understand that I am responsible for changing my password, and I will report the incident to the HSC HIPAA security officer or the UNMH IT Security Office.
- I understand that remote access connections are logged and subject to the same security standards and controls as the internal network. This includes network monitoring, packet capture, web filtering and other security controls.
- I understand that peer-to-peer programs, traffic anonymizers, third-party proxies and other similar systems are not considered secure, and use of these applications over VPN may result in the HSC denying my access to VPN or disabling my HSC accounts.
- I attest that I am personally responsible for any access to sensitive systems that occur from my VPN sessions. I understand that printing patient or sensitive information, including screen shots, could result in HIPAA violations, especially if they are printed to an inappropriate location or not handled according to regulatory requirements.
- I understand that I will not be able to access my local network resources while connected to the VPN. Split tunneling and similar capabilities are not supported by the VPN software.
- I understand that VPN access is for single user access only. Shared accounts and service accounts should not be used with the VPN.
- I understand that UNMH and HSC IT support the VPN Gateway and its client software, but they do not support hardware on my personal computer or external Internet connections to the hospital. Issues I experience with PC hardware or my Internet Service Provider at home are my responsibility to resolve. Therefore, UNMH does not guarantee my ability to access UNMH data or my speed of access.
- I understand that, although VPN service is offered 24/7, the UNMH and HSC service desks will address questions about, and issues with, individual access during their respective service-desk hours. They will handle after-hours issues during normal business hours, unless the issue is systemwide. If at any time I am unable to access the VPN, I will revert to the process I used before I was given this ability.

I have read and agree to the terms and conditions listed in the UNM Health System Virtual Private Network (VPN) Access Authorization for Remote Network Access form.

I understand that maintaining the confidentiality of confidential and restricted information is a requirement of my position, job or a contractual duty with HSC and I also will not access information outside of the role of my position.

Name: ____________________________ Date: ________________

Signature: ____________________________