DEFINITIONS

"Virtual Private Network" or "VPN" is a method to allow secure remote access across the Internet by using encryption and other security mechanisms to ensure that only authorized users can access the network and that data cannot be intercepted.

STANDARD

1) Valid encryption processes for remote access across the Internet are those which comply, as appropriate, with NIST Special Publications 800-52 Rev. 2, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations; 800-77r1, Guide to IPsec VPNs; or 800-113, Guide to SSL VPNs, or others which are Federal Information Processing Standards (FIPS) 140-2 validated.

2) UCLA Health IT SSL VPN and MyDesktop, both with multifactor authentication, are the only methods individual Health Sciences Workforce members may use for remote access to UCLA Health Sciences networks.

3) The following categories of workforce members must not be allowed permissions to use SSL VPN for remote access or to access CareConnect remotely:
   a) UCLA Health Sciences volunteers
   b) UCLA undergraduate students working on projects in the Health Sciences for class credit
   c) Also see HS policy No. 0361, "Clinical Research Volunteers Scope of Duties."

4) Vendors must use UCLA Health SecureLink for remote access by individuals.
   a) If vendors have not yet been set up with SecureLink access, UCLA Health staff may invite vendor support staff to supervised UCLA Health Zoom sessions for just-in-time help with urgent issues.
   b) If vendors have their own SecureLink implementation, a Nexus connection may be configured between their SecureLink and the UCLA Health SecureLink.

5) Approved remote access solutions for external entities or groups of individuals when individual remote access is not the preferable solution will be UCLA Health IT-supported remote access solutions including but not limited to, Business-to-Business VPN, Metro Ethernet connections and remote access appliances.

6) VPN users will be automatically disconnected after no more than two hours of inactivity and will be required to logon again to reconnect. Pings or other artificial network processes are not to be used to keep the connection open. The maximum VPN session length is 15 hours.

7) Firewalls must be implemented for open, unfiltered connections between UCLA Health Sciences networks and external sites (e.g., Metro Ethernet).

QUESTIONS

1) If you have questions on how to use remote access or obtain remote access privileges for individuals, please contact your IT Support Group.
2) If you have questions on how to obtain remote access for entities or groups, please contact ISS Network Security (mccsnetsec@mednet.ucla.edu) or submit a Service Now ticket.
3) If you have questions about this Standard, please contact the Office of Compliance Services – Information Security (CompOffice@mednet.ucla.edu)

REFERENCES

HS Policy No. 9453D, "*Remote Access*"

CONTACT

Chief Compliance Security Officer, Office of Compliance Services

REVISION HISTORY

Created Date: September 25, 2016
Revised: July 31, 2017; August 29, 2017; February 6, 2018; October 16, 2020