DEFINITIONS

"*Multifactor Authentication*" requires a user to provide more than one kind of Authentication Credential to be allowed access to a system. In general, this would be at least two of the following: something you know (a password), something you have (a secure token) and something you are (a biometric identifier such as a fingerprint). Requiring at least two types of authentication provides protection if one credential is compromised.

STANDARD

1) Multifactor Authentication must be used for:
   a) All Mednet Active Domain Administrator access.
   b) All Administrative access to servers that store Protected Health Information.
2) Multifactor Authentication is strongly recommended for Administrative access to all other critical infrastructure and system.
3) Multifactor Authentication should be used for all remote access that does not pass through the UCLA Health VPN to critical systems and systems containing Restricted Information.

QUESTIONS

1) If you have questions on how to use or obtain Multifactor Authentication, please contact your IT Support Group.
2) If you have questions about this Standard, please contact the Office of Compliance Services – Information Security (compoffice@mednet.ucla.edu)

REFERENCES

HS Policy No. 9452, "User Accounts (Authorizing Access to Restricted Information; Passwords)

CONTACT

Chief Compliance Security Officer, Office of Compliance Services

REVISION HISTORY

Created Date: August 3, 2016
Revised: October 16, 2020