## STANDARD

The following standards apply to all devices owned and/or operated by UCLA Health Sciences, as well as any devices which connect to any UCLA Health Sciences network or access UCLA Health Sciences Electronic Information Resources from any location.

**All Devices must comply with the following:**

1) All devices must follow the requirements of HS Policy No. 9457, "*Minimum Security Standards*."

2) All UCLA Health IT-supported systems must comply with the UCLA Health IT Hardening Standards (see the *UCLA Health Vulnerability Management Standard*) and use UCLA Heath IT standardized images. Personally owned systems should comply with the Hardening Standards.

3) Services and applications that will not be used must be disabled.

4) Once Restricted Information (including but not limited to PII and PHI) has been transferred from an endpoint device (including but not limited to workstations, laptops, tablets, and medical devices) to a centralized system such as a designated server, that data should be securely removed from the device unless there is a business need to keep it there.

5) Servers must be located in physically secure access-controlled environments.

6) Servers should be located in secure network zones as appropriate for the data involved.

7) Trust relationships between systems are a security risk and should only be used for approved business cases.

8) Remote administration of servers, workstations, and other systems shall be performed over encrypted channels.

9) Any access to Restricted Information on systems must follow the requirements of HS Policy No. 9452, "*User Accounts*."

10) Configuration changes for production servers must follow the appropriate change control procedures.

**In addition, publicly accessible devices and applications must comply with the following:**

11) Requests for new Mednet public IP addresses or for additional open ports for existing public IP addresses must be approved by the Chief Information Security Officer or designee.

12) The device should be located in a DMZ that limits ingress/egress from the Internet and internal networks to only the necessary network traffic.

13) The Device should have an appropriate Internet Domain name (for example, www.mednet.ucla.edu or www.uclahealth.org) that meets the requirements of UCLA Policy 411, "*Registration and Use of UCLA Domain Names.*"

14) All publicly accessible Mednet web services or RESTful APIs must be configured to use approved UCLA Health IT Web Application Firewalls (WAFs).

15) The device must not provide gateway or proxy services or have network interfaces to multiple subnets.

16) Administration of a Device from outside of Mednet must be performed in compliance with HS Policy No. 9453-D, "*Remote Access*."

**EXCEPTIONS**

1) Exceptions for systems that cannot meet the technical requirements above may be granted by the UCLA Health Sciences Chief Information Security Officer in consultation with the Office of Compliance Services and UCLA Health IT stakeholders.
2) All exceptions must be documented.

**QUESTIONS**

1) For information on Device configuration or vulnerability patching, please contact Customer Care at 310-26**7-CARE** (2273).
2) To obtain copies of the hardening standards or request an exception, please contact IT Security (ITSecurityAll@mednet.ucla.edu).
3) For questions on this standard, please contact the Office of Compliance Services – Information Security (CompOffice@mednet.ucla.edu).

**REFERENCES**

HS Policy No. 9452, "*User Accounts*"
HS Policy No. 9453-D, "*Remote Access*"
HS Policy No. 9456, "*Physical Security of Restricted Information*"
HS Policy No. 9457, "*Minimum Security Standards*"
UCLA Policy 411, "*Registration and Use of UCLA Domain Names*"

**CONTACT**
Chief Privacy and Data Security Officer, Office of Compliance Services

**REVISION HISTORY**
Created Date: May 18, 2019
Updated Date: June 29, 2021