STANDARD

This standard prohibits access to UCLA Health Sciences networks via unsecured wireless communication methods and covers any type of device (e.g., personal computers, cellular phones, tablets, instrumentation, medical devices, etc.) connecting via wireless networking to UCLA Health Sciences networks.

1) UCLAHealthSecure is the preferred wireless solution for end-user devices where it is available. If it is not available in a location, contact UCLA Health IT to learn about other possible approved options.

2) For wireless connectivity for instrumentation or medical devices, contact UCLA Health IT.

3) ALL wireless networks in UCLA Health Sciences locations must be managed by UCLA Health IT.

4) Any unauthorized wireless access point (WAP) may be blocked from UCLA Health Sciences networks without prior warning.

5) Peer-to-peer wireless network capabilities on wireless clients should be disabled, unless such functionality meets an approved business need.

6) Bluetooth devices (headsets, keyboards, mice, printers)
   a) To minimize the risk of compromise via Bluetooth, users should follow the recommendations below:
      i) Turn Bluetooth off when you are not using it. Enable Bluetooth functionality only when necessary.
      ii) Require and use only devices with low-power Class 2 or 3 Bluetooth transceivers.
      iii) Keep devices as close together as possible when Bluetooth links are active.
      iv) Independently monitor devices and links for unauthorized Bluetooth activity.
      v) Make devices discoverable (visible to other Bluetooth devices) only if/when absolutely necessary.
      vi) Make devices connectable (capable of accepting and completing incoming connection requests) only if/when absolutely necessary and only until the required connection is established.
      vii) Pair Bluetooth devices in a secure area using long, randomly generated passkeys. Never enter passkeys when unexpectedly prompted for them.
      viii) Maintain physical control of devices at all times. Remove lost or stolen devices from paired device lists immediately.

ix) Keep your devices up to date on operating system version and security patches.
x) Use device firewalls, and keep device anti-virus software up to date.

b) Bluetooth on any device may not be used if causing interference with existing wireless or other equipment, especially in patient care environments
c) Any use of Bluetooth with clinical equipment must be approved in advance by the UCLA Health Sciences Chief Information Security Officer.

EXCEPTIONS
Any exceptions from this standard must be approved by the UCLA Health Sciences Chief Information Security Officer.

QUESTIONS

1) Contact Customer Care at 310-267-CARE (2273) for any wireless networking needs you may have.
2) Contact IT Security (ITSecurityAll@mednet.ucla.edu) for exception requests.
3) If you have questions about this Standard, please contact the Office of Compliance Services – Information Security (InfoSecAll@mednet.ucla.edu).

REFERENCES
HS Policy No. 9457, "*Minimum Security Standards*"

CONTACT
Chief Compliance Security Officer, Office of Compliance Services

REVISION HISTORY
Created Date: May 18, 2019