MINIMUM SECURITY STANDARDS FOR NETWORK DEVICES

PURPOSE
The purpose of this policy is to outline the required technical standards and minimum configuration for all workstations, servers, and Networking Equipment connected to the UCLA Health System and David Geffen School of Medicine at UCLA (hereafter referred to as “UCLA Health”) networks, along with the standards for connecting to MedNet wirelessly. The policy will be updated as technology and circumstances change. These standards are intended to protect the confidentiality, integrity and availability of Restricted Information for patient care and business purposes.

DEFINITIONS
“Protected health information” or “PHI” is any individually identifiable health information, in any format, including verbal communications. “Individually identifiable” means that the health or medical information includes or contains any element of personal identifying information sufficient to allow identification of the individual, such as the patient’s name, address, electronic mail address, telephone number, or social security number, or other information that, alone or in combination with other publicly available information, reveals the individual’s identity. PHI includes patient billing and health insurance information and applies to a patient’s past, current or future physical or mental health or treatment.

“Electronic Protected Health Information” or “ePHI” is PHI that is transmitted by electronic media or is maintained in electronic media. For example, ePHI includes all data that may be transmitted over the Internet, or stored on a computer, a CD, a disk, magnetic tape or other media.

“Personal Information (PI)” as used in this policy is an individual’s first name or first initial and last name combined with any one of the following:

1. social security number,
2. driver’s license number or California identification card number,
3. account number, credit, or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account,
4. medical information, or
5. health insurance information.

“Medical Information” means any information, in either electronic or physical form, regarding an individual’s medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional, and which may be in the possession of or derived from a health care provider, health care service plan, pharmaceutical company or contractor. “Health insurance information” means an
individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records. Medical information and health insurance information for patients are also considered to be PHI.

“Restricted Information” (as defined by UC Policy IS-3, Electronic Information Security) describes any confidential or Personal Information that is protected by law or policy and that requires the highest level of access control and security protection, whether in storage or in transit. This includes Personal Information, PHI and ePHI as defined in this section but could also include other types of information such as research data.

“Account” is an identity used to gain access to a particular computer, system or application.

“Authorized Personnel” means the designated IT support person or group for an area. For MITS-supported Hospital areas, this would be MITS; for other departments, it would be the departmental CSC; for areas supported by SOMITS, it would be SOMITS. This also includes Office of Compliance Services - Information Security staff.

“CSC” is an abbreviation for Computer Support Coordinator. For the purpose of this policy, this includes any person or group responsible for supporting any Device connected to MedNet.

“Device” means a computer, printer, wireless appliance, or other piece of equipment that can connect to and communicate over any UCLA network. Devices would include, but are not limited to, laptops, PDAs, web servers databases file and other application servers, and medical and other devices with network connectivity.

“MITS” is an abbreviation for Medical Information Technology Services. MITS provides central IT services, including networking, for UCLA Health in cooperation with local departmental IT support groups.

“MedNet” is the data network connecting the UCLA Medical Centers, the School of Medicine and the Community Physician Network.

“MedNet DMZ” is a separate Mednet network zone that provides a higher level of security by restricting access both to and from devices in the zone.

“Networking Equipment” means devices that facilitate the use of computer networks, including, but not limited to, routers, switches, bridges, firewalls, intrusion prevention systems, gateways, VPN, wireless access points and other network appliances.
“Password” is an authorized user’s unique combination of numbers, letters, and/or symbols created by the user and used to securely access the UCLA Health computer, network or e-mail resources.

“Privileged accounts” are accounts with unrestricted access, such as Administrator and Super User accounts.

“Publicly accessible” means a Device that is accessible from the Internet.

“Server” is a Device that provides some service for other Devices connected to it via the network.

“SOMITS” is an abbreviation for School of Medicine IT Services. SOMITS works with MITS to provide networking and other IT support to the School of Medicine.

“User” is anyone who holds a valid account on a UCLA Health network, computer, remote access and/or e-mail system.

“Workstation” is defined for the purposes of this policy as a UCLA Health desktop or laptop computer.

POLICY

I. All publicly accessible Devices attached to the UCLA Health network (MedNet) must be registered with MITS or SOMITS.

II. Publicly accessible Devices should be located in an access-controlled environment when possible.

III. All Devices connecting to UCLA Health networks must be configured according to the relevant standards outlined in this document.

IV. Devices that cannot be protected in the required manner (virus scanning, spyware/adware protection, patch updates, secure configuration) must be located in protected subnets or isolated by other approved means. Such systems would include, but would not be limited to, turn-key systems on which the vendor prohibits any 3rd party software and operating system patches and legacy systems that cannot be updated.

V. All Devices that contain Restricted Information, including, but not limited to PCs, laptops, workstations and PDAs, must be secured with a password-protected screen saver with the automatic activation feature set at 15 minutes or less or by logging off when the Device will be unattended. Screen-saver timeouts longer
than 15 minutes must be approved by the Chief Information Security Officer. Exceptions may be requested by submitting the Timeout Exception Form which can be found at:

VI. All Devices that are connected to a UCLA network, whether owned by UCLA or others, shall be continually executing approved virus-scanning software with current virus definitions. Exceptions must be approved by the Chief Information Security Officer or his/her designee.

VII. Network scanning is expressly prohibited unless prior notification to MITS or SOMITS is made. Some exceptions may be allowed for IT administrative functions that require port scanning (patch and virus update servers, security, inventory) only from registered IP addresses by Authorized Personnel. Exceptions must be approved by Authorized Personnel and scanning across subnets should be kept to a minimum.

VIII. Individuals must not monitor network traffic to intercept data not meant for them unless this activity is a part of their normal job function.

IX. Where appropriate, UCLA Health shall install firewalls and intrusion detection software to reduce the threat of unauthorized remote access.

X. UCLA Health shall run versions of operating systems and application software for which security patches are made available in a timely manner on network Devices. All Devices must be protected against malicious software, such as computer viruses, Trojan horses, spyware, etc. For Devices with operating systems that cannot be updated, cannot be retired and are necessary for ongoing business operations or patient care needs, an exception for continued use of the system must be obtained from the UCLA Health Chief Information Security Officer.

XI. UCLA Health shall where possible terminate web or other application sessions after a short period of inactivity no longer than 15 minutes.

XII. UCLA Health should implement procedures to ensure regular review of log-in attempts and system activity, including reports of any discrepancies. See HS Policy No. 9462, “Privacy and Information Security Auditing and Monitoring.”

XIII. Devices that include native host-based firewall software in the operating system should have the firewall activated and properly configured. Exceptions may be made when the firewall software compromises the usability of critical applications.
XIV. To prevent password harvesting, passwords must not be sent in clear text and all Devices must use encrypted authentication mechanisms or other secure authentication mechanisms. Passwords or protocols which provide no logon access to the system (e.g., anonymous FTP) are exempted from this requirement.

XV. Restricted Information transmitted over the Internet or wireless networks should be encrypted.

A. Any files or attachments containing Restricted Information should be encrypted using 128-bit (or longer) AES.

B. Any transmission method (SSL, HTTPS, SFTP) should use FIPS 140-2 compliant encryption

C. Any exceptions must be approved by the Chief Information Security Officer.

(See: Office for Civil Rights, “Guidance to Render Unsecured Protected Health Information Unusable, Unreadable or Indecipherable”).

XVI. In order to maintain the integrity of UCLA Health networks, any Device which has been compromised or attempts to compromise any other Device may be disconnected from the network without prior warning. The local CSC must be informed of the compromise and disconnection as soon as possible so that the users of the system can be notified and remedial actions can be initiated.

PROCEDURES

I. Device Security

The following standards apply to all Devices owned and/or operated by UCLA Health, and to Devices connected to any UCLA Health network. Devices that are publicly accessible must also comply with the publicly accessible Devices section of this policy.

The standards establish requirements for the base configuration of Devices that are owned and/or operated by UCLA Health to minimize unauthorized access to Restricted Information and electronic resources, and to significantly reduce the threat that non-compliant Devices could have to the integrity of UCLA Health networks and other internal Devices.

Ownership and Responsibilities

A. Departmental management is responsible for ensuring that all Devices have clear ownership and have an identified CSC. These CSCs are
responsible for system administration and should monitor configuration compliance.

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

C. The responsibility of maintaining inventory records of computing equipment will be at the departmental level.

D. The configuration of all Devices must comply with Appendix I – Device Configuration Standard.

E. All security-related events on servers and workstations that contain Restricted Information must be logged and audit trails saved as follows:
   i. All security-related logs should be kept online for a minimum of 4 weeks.
   ii. Backups of security logs should be retained for a minimum of 18 months.

F. The CSCs should routinely review security-related logs.

G. Significant security-related events must be reported to the Office of Compliance Services - Privacy and Information Security (PrivacyInfoSec@mednet.ucla.edu). See HS Policy No. 9459, “Privacy and Information Security Incident Reporting.”

H. All Devices connecting to UCLA networks must also comply with UCLA Policy No. 401, “Minimum Security Standards for Network Devices.”

II. Publicly Accessible Devices

Publicly accessible Devices are vulnerable to attack from the Internet. All publicly accessible Devices owned and/or operated by UCLA Health (including servers, workstations, etc.) should comply with the standards listed below. This section also covers any publicly accessible Devices outsourced or hosted at external or third-party service providers. Note, for the most part, publicly accessible Devices will be servers in a MedNet DMZ.

Ownership and Responsibilities

A. All publicly accessible Devices should be registered with the designated IT support group. The following information should be submitted to positively identify the point of contact in case of an issue:
i. Contact information for the primary and backup system administrator for the Device
ii. DNS name of the Device
iii. IP address of the Device
iv. Operating system information
v. Protocols that the Device will be servicing (i.e. FTP, SMTP, HTTP, HTTPS, POP3)
vi. A description of the main functions/applications/service that the Device will be providing (e.g. “a website for the general public describing our department”).

B. A bi-annual review must be done of open ports for publicly accessible systems. Results will be reviewed with system owners to verify that the systems and ports still need to be publicly accessible. System owners will be responsible for following up on any necessary changes. Any changes and the final status will be documented and reported to the Chief Information Security Officer.

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

D. 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.”

E. Changes to existing Devices and deployment of new Devices should follow change control processes/procedures.

F. The configuration of all publicly accessible Devices must comply with Appendix II – Publicly Accessible Device Configuration Standard.

G. Any web sites, applications or services should be tested for vulnerabilities before going live and should be retested after any changes.

H. If any of the following will be stored or transmitted to or from the Device then it should be connected solely to the MedNet Restricted Information DMZ:
   i. Restricted Information
   ii. Privileged usernames and passwords (i.e. accounts that have access to other internal Devices)
   iii. Personal information (SSN, home addresses, DOB, etc.)
   iv. Confidential University information
III. Networking Equipment

This section describes the required minimal security configuration for all Networking Equipment used in a production capacity at or on behalf of UCLA Health. All Networking Equipment connected to UCLA Health production networks must comply with this section. Networking equipment that is isolated from production networks is not affected. The configuration of all Networking Equipment must comply with Appendix III – Networking Equipment Configuration Standard.

IV. Wireless Communication

This section prohibits access to MedNet via unsecured wireless communication mechanisms. Only wireless systems that meet the criteria of this section or have been granted an exception by the Chief Information Security Officer in consultation with the appropriate IT groups are approved for connection to MedNet.

This section covers all wireless data communication Devices (e.g., personal computers, cellular phones, PDAs, etc.) connected to MedNet. This includes any form of wireless communication device capable of transmitting packet data. Wireless devices and/or networks without any connectivity to MedNet do not fall under the purview of this section, except that any data streams containing Restricted Information would still require encryption. To comply with this section, a wireless device must:

A. Maintain encryption per MedNet standards (see Appendix IV).
B. Not be connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.
C. Adhere to all policies in Appendix IV – Wireless Communication.

V. Enforcement

Failure to follow any provisions of this policy may result in disciplinary action, up to and including termination.

VI. Questions

Workforce members should consult their IT support group or the Office of Compliance Services - Information Security (InfoSecAll@mednet.ucla.edu) if they have any questions on this policy.

VII. Policy Exceptions
Unless an exception process is specified elsewhere in this policy, any exceptions to this policy must be for a valid patient care or business reason and must be approved by the Chief Compliance Officer or his/her designee. The Chief Compliance Officer or designee will consult with the appropriate business, leadership and IT groups in evaluating any proposed exceptions. The exception request form can be found at [http://compliance.uclahealth.org/workfiles/PDF2/HIPAA%20Privacy/HIPAA%20Forms/General%20Exception%20Request%20form.pdf](http://compliance.uclahealth.org/workfiles/PDF2/HIPAA%20Privacy/HIPAA%20Forms/General%20Exception%20Request%20form.pdf)

REFERENCES
Health Insurance Portability and Accountability Act, 45 CFR Sections 160-164
Business & Finance Bulletin IS-3, Electronic Information Security
[http://www.ucop.edu/ucophome/policies/bfb/is3.pdf](http://www.ucop.edu/ucophome/policies/bfb/is3.pdf)
UC Electronic Communications Policy
[http://www.ucop.edu/ucophome/policies/ec/](http://www.ucop.edu/ucophome/policies/ec/)
UCLA Policy No. 401, “Minimum Security Standards for Network Devices”
Office for Civil Rights, “Guidance to Render Unsecured Protected Health Information Unusable, Unreadable or Undecipherable”
NSA Bluetooth Security Recommendations

CONTACT
Chief Privacy Officer, Office of Compliance Services
Chief Information Security Officer, Office of Compliance Services

REVISION HISTORY
Effective Date: April 20, 2005
Approved Date: February 22, 2006
Review Date: July 25, 2012
APPROVAL
Health Sciences Enterprise Compliance Oversight Board
Approved 12/11/2010, 06/27/2012

David Feinberg, M.D.
CEO and Associate Vice Chancellor
UCLA Hospital System

Randolph Steadman, M.D.
Chief of Staff
Ronald Reagan UCLA Medical Center

Denise Sur, MD
Chief of Staff
Santa Monica-UCLA Medical Center and Orthopaedic Hospital

Ian A. Cook, M.D.
Chief of Staff
Resnick Neuropsychiatric Hospital at UCLA
APPENDIX I – DEVICE CONFIGURATION STANDARD

All Devices must comply with the following configurations:

1. Operating System configuration should be in accordance with approved UCLA Health guidelines. Standardized, secured configurations that have been tested and reviewed should be used.

2. Services and applications that will not be used must be disabled.

3. All patches and hot-fixes recommended by hardware vendors, software vendors, MITS or SOMITS must be installed as soon as possible, and no later than three months after their release. This applies to all services installed, even though those services may be temporarily or permanently disabled. The CSC must have processes in place to keep Device current on appropriate patches/hotfixes. Patches/hotfixes deemed critical by MITS or SOMITS must be applied within seven business days of notification being given. Systems that cannot be patched must be in isolated subnets. Any exceptions must be approved by Authorized Personnel.

4. Trust relationships between systems are a security risk, and should only be used when necessary.

5. Always use standard security principles of least required access to perform a function.

6. Do not use privileged accounts (e.g. root or Administrator) when a non-privileged account will do.

7. A disk duplication process should be used for workstations wherever possible (e.g. Symantec Ghost) to ensure standard, secure configurations.

8. The operations group should exhaustively test the original image before it is cloned and used on production workstations.

9. Authorized Personnel must be granted the ability to review the image for potential security issues.

10. Servers should be located in a physically access-controlled environment. Servers are specifically prohibited from operating from uncontrolled areas.

11. Access to services on servers should be logged and/or protected through access-control methods, if possible.
APPENDIX II – PUBLICLY ACCESSIBLE DEVICE CONFIGURATION STANDARD

All publicly accessible Devices must comply with the following configuration:

1. The Device must be in compliance with the Device configuration standard found in Appendix I.
2. The Device should be connected to the MedNet DMZ allocated to the IT support group. If Device will store or transmit Restricted Information, it should be connected to the MedNet confidential data DMZ.
3. The Device should not be part of the standard MedNet network.
4. The Device must not provide gateway or proxy services or have network interfaces to multiple subnets. Any exceptions must be approved by Authorized Personnel.
5. All critical patches and hot-fixes recommended by hardware vendors, software vendors, MITS or SOMITS must be installed as soon as possible, and no later than one month after their release.
   a. All relevant updates must be installed, including updates to services that may be temporarily or permanently disabled.
   b. The CSC must have processes in place to ensure all devices remain current on the appropriate updates.
   c. Patches/hotfixes deemed critical by MITS or SOMITS must be applied within 24 hours of notification.
6. Services and applications that are unnecessary must be disabled (e.g. FTP, Telnet, etc.).
7. For the MedNet confidential data DMZ only 128-bit or greater AES or 3DES SSL connections will be permitted from the external Internet.
8. For all other DMZs, only requested protocols from the following list will be permitted in from the external Internet unless an exception is made by the Chief Information Security Officer in consultation with the appropriate IT groups:
   a. FTP services
   b. HTTP services
   c. HTTPS services
   d. Mail services (POP3, SMTP, IMAP4)
   e. SSH2 (must use a port above 1024)
   f. ICMP (echo, echo reply, destination unreachable, time exceeded)
9. Devices within a DMZ will not be permitted to initiate connections out to the Internet. Exceptions will be granted on a case-by-case basis by the Chief Information Security Officer working in consultation with the appropriate IT groups and documented accordingly.
10. A Device within a DMZ should have minimum connectivity back into the internal MedNet.

11. Administration of a Device from outside of MedNet must be performed via a VPN connection as described in HS Policy No. 9453-D, “Remote Access.”

12. Security-related events should be logged and audit trails saved in accordance with the Device security section of this policy. Security-related events include (but are not limited to) the following:
   a. User login success and failures.
   b. Success and failures to obtain privileged access.
   c. Access policy violations.

13. If there are concerns about the security configuration of a publicly accessible Device, Authorized Personnel must be allowed to perform a security/application audit.
APPENDIX III – NETWORKING EQUIPMENT CONFIGURATION STANDARD

1. Whenever possible, centralized authentication (TACACS+ for Cisco systems) should be implemented.

2. All passwords on the Networking Equipment must be kept in a secure encrypted form. The Networking Equipment must have all passwords set to the current production password from MITS Network Services unless exclusively controlled by a School of Medicine department.

3. Disallow the following when appropriate
   a. IP directed broadcasts
   b. Incoming packets at the router sourced with invalid addresses
   c. TCP small services
   d. UDP small services
   e. All web services running on Networking Equipment

4. Use MITS standardized SNMP community strings, unless exclusively controlled by a School of Medicine department. SNMP strings should be set using the same rules as for strong passwords.

5. Access rules are to be added as business needs arise.

6. Networking Equipment that is exclusively controlled by a School of Medicine department must be registered with MITS or SOMITS with a designated point of contact.

7. Networking Equipment should be physically located in an access-controlled environment. Routers are specifically prohibited from operating from uncontrolled cubicle areas.

8. Use of end-user-deployed routers, switches, VPN and other gateways, and wireless access points is prohibited unless approval has been obtained in advance from Authorized Personnel.
APPENDIX IV – WIRELESS COMMUNICATION CONFIGURATION STANDARD

1. All wireless communications solutions that provide connections to UCLA Health internal networks must use approved wireless encryption technology:
   a. Centrally-managed Mednet Wireless Networking (MWN) services
      i. Mednet WiFi
      ii. Mednet Wireless. Users must encrypt all wireless traffic via a connection to a Mednet VPN concentrator.
   b. Users of departmentally configured Wireless Access Points (WAP) must either encrypt all wireless traffic via a connection to a Mednet VPN concentrator or obtain approval for alternative encryption methods from the Chief Information Security Officer.

2. No wireless access points (WAP) that conflict with MWN services will be permitted. Conflicting devices will be disabled until the interference issues can be resolved.

3. Where MWN service is not available, authorized IT staff (and only authorized IT staff) may set up local WAPs as per requirements below.
   a. Local WAPs must have a static IP address that must be registered with MITS or SOMITS along with the WAP location and contact information.
   b. Before installing local WAPs near any clinical areas, a spectral analysis must be performed to ensure there will be no interference that could affect patient care.
   c. WAPs near clinical areas must have power levels set to less than 50 milliwatts.
   d. WAPs that do not meet the requirements above must be approved by the Chief Information Security Officer working in consultation with the appropriate IT groups.

4. Bluetooth devices (headsets, keyboards, mice, printers)
   a. To minimize the risk of compromise via Bluetooth, users should follow the recommendations below:
      i. 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.

ix. Use device firewalls, regularly patch Bluetooth devices, 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

5. Any use of Bluetooth with clinical equipment must be approved in advance by the UCLA Health Chief Information Security Officer.