

INFORMATION TECHNOLOGY SECURITY

PURPOSE

The purpose of this policy is to outline the required technical standards and minimum configuration for all workstations, servers, routers and switches connected to the UCLA Health System network (Mednet), along with the standards for connecting to MedNet wirelessly or from a remote location. The policy will be updated as technology and circumstances change. These standards are intended to protect the confidentiality, integrity and availability of ePHI for patient care and business purposes.

DEFINITIONS

Term	Definition
<i>Authorized Personnel</i>	The designated IT support person or group for an area. For Hospital areas, this would be MCCS; for SOM departments, it would be the departmental CSC; for areas supported by SOMITS, it would be SOMITS.
<i>Confidential Information</i>	Confidential information includes but is not limited to: protected health information (PHI), research data, proprietary business and corporate strategic information, competitor sensitive information, trade secrets, specifications, and legally privileged information.
<i>CSC</i>	Computer Support Coordinator. For the purpose of this policy, this includes any person or group responsible for supporting any host connected to MedNet
<i>External host</i>	A host on the outside of the MedNet perimeter firewall.
<i>Firewall</i>	A security design that prevents unauthorized users from gaining access to MedNet
<i>Host</i>	A TCP/IP-based device (e.g., PC, server, printer)
<i>Internal host</i>	A host on the inside of the MedNet Internet firewall. This does not include hosts connected to other campus networks.
<i>MCCS</i>	Medical Center Computing Services
<i>MedNet</i>	The data network connecting the UCLA Medical Centers, various School of Medicine departments and the Primary Care Network.
<i>MedNet DMZ</i>	A secure network segment of MedNet that contains hosts which: <ul style="list-style-type: none"> • may not initiate a connection to an internal host except for necessary approved connections to internal services. (E.g. a web server may need to communicate back to an internal database or to a mail gateway.) • will accept connections that initiate from an internal or external host • may initiate connections to an external host on a restricted basis.

<i>Network Security Task Force</i>	A group consisting of representatives from MCCS, SOMITS and the School of Medicine CSCs that works together to propose network security policies and resolve network security issues.
<i>PHI</i>	Protected Health Information is an individual's health information that: <ul style="list-style-type: none"> • Is created or received by a health care provider, plan or clearinghouse; • Relates to the past, present or future physical or mental health or condition of an individual, the provision of health care to the individual, or the past, present or future payment for the provision of health care to the individual; • Identifies the individual, or is reasonably believed could identify the individual; and • Is transmitted or maintained in any form or medium. (Definition from the HIPAA UC Systemwide Standards, see http://www.hhs.gov/ocr/regtext.html for the official HIPAA Final Privacy Rule regulation text.)
<i>ePHI</i>	Any electronic PHI that is created, received, maintained or transmitted in electronic format. For example, ePHI may be transmitted over the Internet, or stored on a computer, a CD, a disk, magnetic tape, or other media.
<i>Privileged accounts</i>	Accounts with system-level access to any host connected to MedNet (e.g. sub accounts, accounts that are member of "administrators" group, etc.)
<i>Production network</i>	A network used in the daily business of the UCLA Medical Sciences. Any network connected to the corporate backbone, either directly or indirectly, which lacks an intervening firewall. Any network whose impairment would result in direct loss of functionality to UCLA Medical Sciences employees or impact their ability to do work.
<i>Publicly accessible</i>	An internal host that is accessible to an external host (from the Internet).
<i>Server</i>	A host that provides some service for other hosts connected to it via the network.
<i>SOMITS</i>	School of Medicine IT Services
<i>Spam</i>	Unauthorized and/or unsolicited electronic mass mailings.
<i>VPN</i>	A Virtual Private Networks allows 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.
<i>VPN concentrator</i>	A device in which VPN connections are terminated.
<i>Workstation</i>	For purposes of this policy, a workstation is defined as an internal UCLA Medical Sciences desktop or laptop machine.

I POLICY

- 1) All publicly accessible servers attached to the UCLA Health System network (MedNet) must be registered with Medical Center Computing Services (MCCS) or SOMITS and should be located in an access-controlled environment when possible.
- 2) All systems connecting to UCLA Health System Electronic Information Resources must be configured according to the relevant standards outlined in this document.
- 3) Systems that cannot be protected in the recommended ways (virus scanning, spyware/adware protection, patch updates, secure configuration) must be located in protected subnets or shielded from MedNet 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.
- 4) All devices that contain confidential information, including, but not limited to PCs, laptops, workstations and PDAs, should be secured with a password-protected screensaver with the automatic activation feature set at 15 minutes or less, or by logging-off when the host will be unattended.
- 5) All hosts used by the employee that are connected to MedNet, whether owned by the employee or the UCLA Medical Sciences, shall be continually executing approved virus-scanning software with a current virus database. Exceptions must be approved by authorized personnel.
- 6) Port scanning or security scanning is expressly prohibited unless prior notification to MCCS 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 and scanning across subnets should be kept to a minimum.
- 7) Executing any form of network monitoring which will intercept data not intended for the employee's host, is prohibited unless this activity is a part of the employee's normal job/duty.
- 8) Where appropriate, UCLA Health System shall install firewalls and intrusion detection software to reduce the threat of unauthorized remote access.
- 9) UCLA Health System shall run versions of operating system and application software for which security patches are made available in a timely manner on networked devices. All devices must be protected against malicious software, such as computer viruses, Trojan horses, spyware, etc.

- 10) UCLA Health System shall where possible terminate electronic sessions after a period of inactivity.
- 11) UCLA Health System shall implement procedures to ensure regular review of log-in attempts and system activity, including a report of any discrepancies.
- 12) If local IT support personnel cannot resolve critical problems that could adversely affect others in the Medical Sciences, the Network Security Task Force may designate a team to advise and assist the local person.

I PROCEDURES - Host Security

The following standards apply to all hosts owned and/or operated by UCLA Health System, and to hosts registered under any UCLA Health System owned internal network domain. This section is specifically for all hosts attached to MedNet. Hosts that are publicly accessible must also comply with the publicly accessible hosts section of this policy.

The standards establish requirements for the base configuration of internal hosts that are owned and/or operated by UCLA Health System to minimize unauthorized access to patient data and proprietary information and technology, and to significantly reduce the threat that compliant hosts will have to the integrity of MedNet and other internal hosts.

Ownership and Responsibilities

1. Department management is responsible for ensuring that all hosts have clear ownership and have an identified CSC. These CSCs are responsible for system administration and should monitor configuration compliance.
2. Configuration changes for production servers must follow the appropriate change control procedures.
3. The responsibility of maintaining inventory records of computing equipment will be at the departmental level.
4. The configuration of all internal hosts must comply with Appendix I – Host Configuration Standard.
5. In order to maintain the integrity of MedNet, any host which has been compromised or attempts to compromise any other host may be disconnected from MedNet without prior warning. The local CSC must be informed as soon as possible so that the users of the system can be notified and remedial actions can be initiated.

6. All security-related events on servers and workstations that contain confidential information must be logged and audit trails saved as follows:
 - a. All security-related logs must be kept online for a minimum of 2 weeks.
 - b. Backups of security logs must be retained for a minimum of 1 year.
7. The CSC should routinely review security-related logs.
8. Significant security-related events will be reported to the designated IT support group, which will review logs and report incidents to the UCLA Medical Sciences management. Prompt notification is always required whenever confidential information may have been compromised. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to: unauthorized access to privileged accounts and denial of service attacks originating from systems. See UCLA Health System Policy No. 9459, "*Security Incident Reporting*."

III Publicly Accessible Host

Publicly accessible internal hosts are particularly vulnerable to attack from the Internet since they receive significantly reduced protection from the MedNet perimeter firewalls. All publicly accessible hosts owned and/or operated by UCLA Health System (including servers, printer, workstations, etc.) must comply with the standards listed below. This section also covers any publicly accessible hosts outsourced or hosted at external/third-party service providers. Note, for the most part, publicly accessible hosts will be servers in a MedNet DMZ.

In order to maintain the integrity of MedNet, any host believed to be compromised may be disconnected from MedNet without prior warning.

Ownership and Responsibilities

1. All publicly accessible hosts must be registered with the designated IT support group. At a minimum, the following information must be submitted to positively identify the point of contact in case of an issue:
 - a. Contact information for the primary and backup system administrator for the host
 - b. DNS name of host
 - c. IP address of host
 - d. Operating system information
 - e. Protocols that the host will be servicing (i.e. FTP, SMTP, HTTP, HTTPS, POP3)
 - f. A description of the main functions/applications/service that the host will be providing (e.g. 'a website for the general public describing our department').

An annual review will be done of servers and open ports.

2. The host must have appropriate Domain Name Server records.
3. Changes to existing hosts and deployment of new hosts must follow change control processes/procedures.
4. The configuration of all publicly accessible hosts must comply with Appendix II – Publicly Accessible Host Configuration Standard.
5. If any of the following will be stored or transmitted to or from the host then it must be connected solely to the MedNet confidential data DMZ, and a secure connection method must be used (see the remote access section of this policy):
 - PHI (protected health information)
 - Privileged usernames and passwords (i.e. accounts that have access to other internal hosts)
 - Personal information (SSN, home addresses, DOB, etc)
 - Confidential University information
6. For equipment outsourced to external service providers, the contracting department is responsible for third party compliance with this policy.

IV REMOTE ACCESS

The following standards must be followed for connecting to MedNet from any external host:

1. The only permitted remote access to MedNet is that which is directed through the MedNet VPN Concentrator, using 128-bit SSL or the MedNet reverse proxy.
2. Approved UCLA Medical Sciences employees and authorized third parties (customers, vendors, etc.) may utilize the benefits of these more secure communication methods. The user is responsible however for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees.
3. It is the responsibility of employees with these privileges to ensure that unauthorized users are not allowed access to MedNet. This includes ensuring that:
 - a) At no time should any UCLA Medical Sciences employee provide their login password to anyone, including family members.
 - b) You must not distribute any VPN configuration files (.PCFs) you are entrusted with.

4. VPN users must be authorized for VPN access by their home departments and must be registered on the online VPN Authorization page. Possession of a VPN configuration file (.PCF) does not confer authorization. Generic accounts (such as those assigned for classroom calendars) may not be used for VPN access.
5. Hardware-based remote access solutions will be set up and managed by authorized IT personnel only.
6. Users are responsible for ensuring that any of their hosts connected to MedNet via a secure method or any other technology are protected by up-to-date anti-virus scanners, and software or hardware firewalls that are configured to protect against attacks from non-MedNet hosts. The software/hardware firewalls must not be disabled during the secure connection. When users are required operationally to temporarily turn off the firewalls to allow remote access for IT support or to run applications that are not firewall-compatible, they must turn the firewalls back on as soon as possible.
7. VPN users will be automatically disconnected from MedNet after 2 hours of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.
8. The maximum VPN concentrator session length is 15 hours.
9. Users of hosts that are not UCLA Medical Sciences-owned equipment must configure the equipment to comply with this policy.
10. Users of hosts that are connected to MedNet via the VPN must comply with the acceptable use section of this policy
11. Only approved VPN software and hardware may be used.
12. No host connected to MedNet via VPN is allowed to serve as a proxy to forward traffic from any other hosts.
13. By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of the UCLA Medical Sciences, and as such are subject to the same rules and regulations that apply to UCLA Medical Sciences-owned equipment, i.e., their machines must be configured to comply with all relevant sections of this policy

V Routers and Switches

This section describes a required minimal security configuration for all routers and switches connecting to a production network or used in a production capacity at or on behalf of the UCLA Medical Sciences. All routers and switches connected to the UCLA Medical Sciences production networks must comply with this section. Routers and switches that are isolated from MedNet are not affected. The configuration of all internal routers and switches must comply with appendix III – Internal router and switch configuration standard.

VI 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 exclusive waiver by M CCS are approved for connectivity to MedNet. Since wireless technology is rapidly evolving, these policies will need to adapt as technology changes.

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 (any PHI-containing data streams would still require encryption). To comply with this section, wireless device must:

1. Maintain point-to-point encryption per MedNet standards (see Appendix IV).
2. Maintain a hardware address that can be registered and tracked (i.e., a MAC address).
3. 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.
4. Adhere to all policies in Appendix IV – Wireless Communication.

REFERENCES

SANS Institute Security Policy Project - <http://www.sans.org/resources/policies/>

UC Electronic Communications Policy - <http://www.ucop.edu/ucophome/policies/ec/>

Business & Finance Bulletin IS-3, Electronic Information Security -
<http://www.ucop.edu/ucophome/policies/bfb/is3.pdf>

Health Insurance Portability and Accountability Act, 45 CFR Sections 160-164

REVISION HISTORY

1st Draft date: December 4, 2002 (individual documents for each section)

2nd Draft date: April 15, 2003 (combined policy)

3rd Draft date: April 25, 2003 (combined server and workstation sections into one host section)

4th Draft date: July 2, 2003 (added DMZ information and replace 'UCLA Health System' with 'UCLA Medical Sciences')

5th Draft date: August 28, 2003 (added Policy – General section and moved the configuration standards for hosts out into appendices)

6th Draft date: March 14, 2005 (revised by Network Security Task Force)

7th Draft date: April 11, 2005 (Document numbered into Compliance Security Policies Series. Section I in Policy No. 9451 "*Use of Electronic Information by UCLA Health System Workforce Members*" and Section II into Policy No. 9457 "*Technical Security*")

Effective Date: April 20, 2005

Approved Date: February 22, 2006

Revised Date: November 2005; June 21, 2007; May 30, 2008

APPROVAL

HIPAA Committee

Hospital Compliance Committee

Carole A. Klove, RN, JD
Chief Compliance and Privacy Officer

APPENDIX I – INTERNAL HOST CONFIGURATION STANDARD

1. All internal hosts must comply with the following configuration:
2. Operating System configuration should be in accordance with approved UCLA Medical Sciences guidelines. Standardized, secured configurations that have been tested and reviewed should be used.
3. Services and applications that will not be used must be disabled where practical.
4. All patches and hot-fixes recommended by hardware vendors, software vendors, MCCS 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 stay current on appropriate patches/hotfixes. Patches/hotfixes deemed critical by MCCS 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.
5. Trust relationships between systems are a security risk, and should only be used when necessary.
6. Always use standard security principles of least required access to perform a function.
7. Do not use privileged accounts (e.g. root or Administrator) when a non-privileged account will do. Avoid the use of generic, shared accounts.
8. A disk duplication process should be used for workstations wherever possible (e.g. Symantec Ghost) to ensure standard, secure configurations.
9. The operation group should exhaustively test the original disk before it is cloned and used on production workstations
10. Authorized personnel must be granted the ability to review the original workstation disk for potential security issues.
11. Servers should be located in a physically access-controlled environment. Servers are specifically prohibited from operating from uncontrolled areas.
12. Access to services on servers should be logged and/or protected through access-control methods such as TCP Wrappers, if possible.

APPENDIX II – PUBLICLY ACCESSIBLE HOST CONFIGURATION STANDARD

1. All publicly accessible hosts must comply with the following configuration:
2. The host must be in compliance with the internal host configuration standard found in Appendix I.
3. The host must be connected to the MedNet DMZ allocated to the support group. If host will store or transmit confidential data it must be connected to the MedNet confidential data DMZ (see IV.C.1).
4. The host must not be part of the standard MedNet network. More specifically, hosts must not be providing gateway or proxy services or have network interfaces to multiple subnets. Any exceptions must be approved.
5. All critical patches and hot-fixes recommended by hardware vendors, software vendors, MCCS or SOMITS must be installed as soon as possible, and no later than one month 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 stay current on appropriate patches/hotfixes. Patches/hotfixes deemed critical by MCCS or SOMITS must be applied within 24 hours of notification being given.
6. If a system is compromised and is a danger to other systems in the DMZ or to internal systems, it may be disconnected from the network.
7. Services and applications that are unnecessary must be disabled (e.g. FTP, Telnet, etc.).
8. For the MedNet confidential data DMZ only 128-bit SSL connections will be permitted from the external Internet.
9. For all other DMZ's, only requested protocols from the following list will be permitted in from the external Internet unless an exception is made by the CIO:
 - FTP services
 - HTTP services
 - HTTPS services
 - Mail services (POP3, SMTP, IMAP)
 - SSH2 (must use a port above 1024)
 - ICMP (echo, echo reply, destination unreachable, time exceeded)
10. The default, more secure, configuration will be not to allow systems within a DMZ to initiate connections out to the Internet. As requested, it will be permitted.
11. By default, systems within a DMZ may only initiate FTP, HTTP or HTTPS connections back into the internal MedNet. Any exceptions must be approved.
12. Administration of the host from outside of MedNet must be performed via a secure method outlined in the remote access section of this policy (i.e. VPN, SSL, or reverse proxy).

13. Security-related events must be logged and audit trails saved in accordance with the host security section of this policy. Security-related events include (but are not limited to) the following:
 - User login failures.
 - Failure to obtain privileged access.
 - Access policy violations.

14. If there are concerns about the security configuration of a publicly accessible host, approved IT personnel must be allowed to perform a security/application audit.

APPENDIX III – INTERNAL ROUTER AND SWITCH CONFIGURATION STANDARD

1. Whenever possible, centralized authentication (TACACS+ for Cisco systems) should be implemented.
2. All passwords on the router must be kept in a secure encrypted form. The router must have all passwords set to the current production router password from MCCA network services unless exclusively controlled by a School of Medicine department.
3. Disallow the following:
 - 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 router
4. Use corporate 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. The router must be registered with MCCA or SOMITS with a designated point of contact.
7. Routers 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 residential routers, gateways and wireless access points is prohibited unless authorization has been obtained in advance.

APPENDIX IV – WIRELESS COMMUNICATION

1. Centrally managed MedNet Wireless Networking (MWN) exists now in many areas of the Medical Sciences. In the future, the MWN will be extended throughout the Medical Sciences. No wireless access points (WAP) that conflict with MWN service will be permitted. Conflicting devices will be disabled until the interference issues can be resolved.
2. MWN users must register the MAC addresses of their wireless devices.
3. MWN users must encrypt all wireless traffic via a connection to the MedNet VPN concentrator.
4. Where MWN service is not available, authorized IT staff (and only authorized IT staff) may set up local WAPs as per requirements below.
 - Local WAPs must be set up on the reserved MedNet SOM wireless subnet and have a static IP address that must be registered with MedNet along with the WAP location and contact information.
 - All users of local WAPs must encrypt all wireless traffic via a connection to the MedNet VPN concentrator (the only traffic allowed out of the SOM wireless subnet will be through the VPN concentrator).
 - CSCs who wish to provide for guest access on their WAPS must have WAPs that handle multiple VLANs (wireless guest access is currently under development).
 - 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.
 - WAPs near clinical areas must have power levels set to less than 50 milliwatts.
5. Bluetooth on any device should be disabled when not in use and cannot be used at all in patient areas or if causing interference with existing wireless or other equipment.