Effective Date:	*04/2005*
Approved Date:	*09/2020*
Revised Date:	*07/2020*
Next Review:	*09/2023*
Owner:	*Liangzhou Chen: Mgr*
Policy Area:	*Compliance*
Reference Tags:	*Lippincott*
Applicability:	*Ronald Reagan, Resnick, Santa Monica, Ambulatory Care*

Minimum Security Standards, HS 9457

PURPOSE

This policy outlines the required technical configuration standards for devices (Workstations, Servers, Networking Equipment, etc.) connecting to UCLA Health Sciences Electronic Information Resources. These requirements are intended to protect the confidentiality, integrity and availability of Restricted Information and for patient care, education, research and other business purposes.

SCOPE

This Policy applies to all faculty, staff, employees, students, trainees, and volunteers of the Ronald Reagan UCLA Medical Center, the Santa Monica UCLA Medical Center and Orthopaedic Hospital, the Resnick Neuropsychiatric Hospital at UCLA, the Faculty Practice Group, all ambulatory clinics and the David Geffen School of Medicine at UCLA (hereafter referred to as "UCLA Health Sciences"). In addition, it applies to suppliers, contractors and other non-workforce members who are allowed access to UCLA Health Sciences Electronic Information Resources or Restricted Information.

POLICY

I. **All devices used by UCLA Health Sciences workforce members to access UCLA Health Sciences Electronic Information Resources, whether owned by UCLA or others, must:**

A. **Be kept up to date on application and operating system supported versions and up to date on security patches**
UCLA Health Sciences shall run versions of operating systems and application software for which security patches are made available in a timely manner.

B. **Use anti-malware software and keep it up to date**
All Devices used by UCLA Health Sciences workforce members, whether owned by UCLA or others, that access UCLA Health Sciences Electronic Information Resources, shall be continually executing approved malware-scanning software with current definitions.

C. **Use a password-protected screen saver that comes up after 15 minutes of inactivity**
All Devices used by UCLA Health Sciences workforce members that access or store UCLA Health Sciences Restricted Information, including, but not limited to PCs, laptops, workstations, smart phones and tablets, must be secured with a password-protected screen saver with the automatic activation feature set at 15 minutes or less or by automatic log off after 15 minutes of inactivity.

D. **Use the host-based firewall**
Devices that include native host-based firewall software in the operating system should have the firewall activated and properly configured.

E. **Run any additional required security software**
Any additional security software specified in the Health Sciences Security Software Standard must also be installed.

F. **Comply with the Health Sciences Standards listed below**:
Health Sciences Vulnerability Management Standard
Health Sciences Device Configuration Standard
Health Sciences Wireless Communications Standard
Health Sciences Data and System Integrity Standard
Health Sciences Network Device Configuration Standard

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

III. To prevent password harvesting, passwords must not be sent in clear text and all devices and applications must use encrypted authentication mechanisms or other secure authentication mechanisms.

IV. Restricted Information transmitted over the Internet or wireless networks must be encrypted according to the Health Sciences Data-in-Motion Encryption Standard.

V. 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.

VI. Where appropriate, UCLA Health Sciences shall install firewalls, intrusion prevention software and other security measures to reduce the threat of unauthorized remote access.

VII. In order to maintain the integrity of UCLA Health Science networks, any Device which has been compromised or attempts to compromise any other Device, may be disconnected from the network without prior warning. The IT Support group 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.

VIII. Devices that do not meet the requirements of this policy and have not been granted exceptions may be blocked from access to UCLA Health Sciences Electronic Information Resources.

IX. UCLA Health IT shall maintain inventories of UCLA-owned computing and network devices.

X. Development and implementation of all new and upgraded systems and applications, and the maintenance and decommissioning of all existing systems and applications, should follow the Health Science Secure System Development Life Cycle Standard.

XI. Risk assessments shall be performed for new devices and applications before initial go live and after any major changes as required by the Health Science Risk Assessment Standard

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

XIII. **Policy Exceptions**
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. To request an exception, fill out this form and email it to compoffice@mednet.ucla.edu.

XIV. **Questions**

A. For information on how to implement these requirements, contact Customer Care at 310-26**7-CARE** (2273).

B. For questions on this policy or to request exceptions, contact the Office of Compliance Services - Information Security (InfoSecAll@mednet.ucla.edu).

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
UC Electronic Communications Policy
http://www.ucop.edu/ucophome/policies/ec/
UCLA Policy No. 401, "Minimum Security Standards for Network Devices"
http://www.adminpolicies.ucla.edu/pdf/401.pdf
Office for Civil Rights, "Guidance to Render Unsecured Protected Health Information Unusable, Unreadable or Undecipherable"
http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html

CONTACT

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

Health Sciences Enterprise Compliance Oversight Board Approved: 12/11/2010, 06/27/2012

APPENDIX I – DEFINITIONS

"Electronic Information Resources" includes, but is not limited to, computer equipment (servers, workstations, laptops and other portable computers), online services, medical devices, mobile devices (tablets ,smart phones, digital cameras, etc.), applications (Electronic Health Record, email, databases, other software), storage media (USB drives, DVDs, CDs, magnetic tape, memory cards), and networks.

"Protected health information" or "PHI" is any individually identifiable health information, in any form or media, whether electronic, paper, or oral. "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, genetic or other information that, alone or in combination with other publicly available information, reveals the individual's identity. PHI includes medical information; 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 means either of the following:

1. An individual's first name or first initial and last name in combination with any one or more of the following data elements when either the name or the data elements are not encrypted:
    A. social security number,
    B. driver's license number or California identification card number,
    C. 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,
    D. medical information, or
    E. health insurance information, or
    F. information or data collected through the use or operation of an automated license plate recognition system as defined in the California Civil Code §1798.90.5; or
2. A user name or email address, in combination with a password or security question and answer that would permit access to an online account

"***Medical Information***" means any individually identifiable 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.

"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.

All revision dates: 07/2020, 06/2019, 08/2012, 03/2011, 05/2008, 06/2007, 11/2005

Attachments

No Attachments

Approval Signatures

Step Description	Approver	Date
Administration Approval- President and CEO, UCLA Health	Johnese Spisso: Ceo Med Ctr [JB]	09/2020
Ronald Reagan Medical Staff Executive Committee- Chief of Staff	Carlos Lerner: Assoc Prof Of Clin-Hcomp [JB]	09/2020
Santa Monica Medical Staff Executive Committee- Chief of Staff	Roger Lee: Hs Clin Prof-Hcomp [JB]	09/2020
Hospital System Policy Committee Chair	Jeffrey Bergen: Mgr [KK]	09/2020
Policy Owner	Liangzhou Chen: Mgr	08/2020