

USE OF ELECTRONIC INFORMATION BY UCLA HEALTHCARE WORKFORCE (EMPLOYEES)

PURPOSE

This policy sets forth guidelines for the use of electronic protected health information (“ePHI”) by UCLA Healthcare Workforce (Employees).

DEFINITIONS

“Electronic Protected Health Information” or “ePHI” is any electronic information that is created or received by a health care provider that relates to the past, present, or future physical or mental health of an individual, and identifies the individual. This includes ePHI that is created, received, maintained or transmitted. For example, ePHI may be transmitted over the Internet, or stored on a computer, a CD, a disk, magnetic tape or other media.

“Workforce” means employees, volunteers, and other persons whose conduct, in the performance of their work for UCLA Healthcare, is under the direct control of UCLA Healthcare or the Regents of the University of California, whether or not UCLA Healthcare pays them. The Workforce includes employees, medical staff, and other health care professionals, agency, temporary and registry personnel, and trainees, housestaff, students and interns, regardless of whether they are UCLA trainees or rotating through UCLA Healthcare facilities from another institution.

POLICY/PROCEDURE

1. **Electronic Information Resources May Only Be Used for UCLA Healthcare Activities**
 - A. UCLA Healthcare Electronic Information Resources, including but not limited to, computer equipment, software, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of UCLA Healthcare and are to be used for the work-related business activities and operations of UCLA Healthcare. These activities include communications with UCLA Healthcare patients, clients, and customers in the normal course of business operations. Incidental personal use of UCLA Healthcare computer resources must comply with University of California policy. (See UC Policy *“Electronic Communications, Section III D.8”*).

- B. All data created using UCLA Healthcare Electronic Information Resources shall remain the property of The Regents of the University of California.
- C. Each UCLA Healthcare department is responsible for creating department-specific guidelines concerning the use of Internet/Intranet/Extranet systems. In the absence of such policies, employees shall be guided by departmental policies on personal use of other resources and if there is any uncertainty, the employee should consult his or her supervisor.
- D. Any activity that is illegal under local, state, federal or international law, or disallowed by University of California policy is strictly prohibited, and may result in disciplinary action in accordance with Compliance Policy No. 9600, *“Responding to Compliance Issues.”*

2. General Requirements; Information for Users

- A. All members of the UCLA Healthcare Workforce who are involved in the creation, transmission and storage of ePHI must receive training about the HIPAA Security Rule (See: Security Policy No. 9460, *Privacy and Security Training and Education Plan.*)
- B. Access to ePHI at UCLA Healthcare is limited to those individuals for whom it is an authorized work-related requirement. (See: Security Policy No. 9452, *“User Accounts: Authorizing ePHI Access by UCLA Healthcare Workforce (Employee) Members): Passwords)*
- A. All members of the UCLA Healthcare Workforce are responsible for ensuring compliance with the UCLA Healthcare policies and safeguards to protect ePHI including, but not limited to: (a) accessing only the amount of ePHI necessary to complete job responsibilities and only for those patients for whom the workforce member needs access to complete job responsibilities; (b) not sharing passwords for computer systems; (c) logging out of computer applications when done; and (d) using different passwords for different computer systems. Authorized users must use a sufficiently complex password to access systems containing ePHI. This password must never be shared. Passwords should be developed in accordance with the policies and procedures described in Security Policy No. 9452, *“User Accounts: Authorizing ePHI Access by UCLA Healthcare Workforce (Employee) Members): Passwords).*
- B. Every precaution must be taken to safeguard user and viewing access to applications that expose confidential information.

- C. Whenever possible, confidential information should either be 1) stored to a network server, 2) de-identified (see: Privacy Policy No. 9440, "*Release of Protected Health Information for Research Purposes*"), 3) removed from electronic data files or 4) encrypted.
- D. All members of the UCLA Healthcare Workforce must secure, maintain and when necessary, dispose of all removable electronic media that may contain ePHI according to established procedures. Removable electronic media includes, but is not limited to, magnetic tapes, portable hard drives, CD-ROMs, DVDs, floppy disks, USB and flash memory cards.
- E. Employees should use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.
- F. Random periodic audits may be conducted as necessary by authorized UCLA Healthcare personnel to ensure the security, privacy, integrity and availability of all UCLA Healthcare data and information systems and compliance with all applicable UCLA Healthcare policies.

Audits may include, but are not limited to, inspections and reviews of:

- a) User and/or system access to any computing or communications device
- b) User access to data and/or information including a review of audit trails
- c) Physical inspections of computer equipment, systems, devices, servers, printers, workstations and other devices
- d) Interactive monitoring and logging of traffic on Mednet
- e) Publicly accessible hosts

Access to equipment and system logs must be granted to authorized personnel upon request. Any suspected or actual inappropriate access by a UCLA Healthcare Workforce member will be investigated and handled in accordance with Compliance Policy No. 9491, "*Specific Audit of Protected Health Information (PHI) Access.*"

- I. The failure of any UCLA Healthcare Workforce member to comply with UCLA Healthcare Security policies, including any departmental security policy and/or procedures, may be subject to disciplinary action in accordance with University personnel policies.
- J. All UCLA Healthcare Workforce members must notify the appropriate supervisory personnel in the event of an actual or suspected security breach. (See: Security Policy No. 9459, "*Security Incident Reporting*").

3. Use of Electronic Information Resources by UCLA Healthcare Contractors and Vendors

No contractor or vendor doing business with UCLA Healthcare shall be permitted access to UCLA Healthcare systems containing ePHI unless the contractor or vendor has first entered into a University-approved contract (describing the services or supplies to be provided by the contractor or vendor and the security measures to be followed in transmitting ePHI between UCLA Healthcare and the contractor or vendor), along with a Business Associate Agreement executed in accordance with Policy No. 9430 *'Business Associates'*. All such contractor and/or vendor access to ePHI shall have defined expiration dates.

The UCLA Healthcare Department Administrator who is the Designated Authorizer for vendors or contractors working in their department must immediately notify the Security Department to revoke access for any contractor or vendor staff member(s) who are no longer employed by the contractor or vendor, as soon as they are aware that the individual(s) is no longer working for them.

4. Unacceptable Uses of Electronic Information Resources

The following uses of Electronic Information Resources are examples of uses that are **prohibited** by UCLA Healthcare policy, unless exempted in writing by designated Security staff as part of a legitimate UCLA Healthcare job responsibility.

- A. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, and copyrighted music.

The installation of any copyrighted software for which UCLA Healthcare or the end user does not have an active license is strictly prohibited.

- B. The exportation of software, technical information, encryption software or technology, in violation of international or regional export control laws. Such activity is illegal and prohibited by UCLA Healthcare policy.
- C. The introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

- D. Revealing an employee-specific account password to others or allowing the use of an employee's account by others. This prohibition also prohibits an employee from sharing passwords with his or her family members or members of his or her household.
- E. Using a UCLA Healthcare computing asset to actively engage in procuring or transmitting material that is in violation of UCLA Healthcare's sexual harassment policies and/or hostile workplace policies, including applicable laws and regulations.
- F. Making fraudulent offers of products, items, or services originating from any UCLA Healthcare account.
- G. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
- H. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties.
- I. Circumventing user authentication or security of any host, network or account.
- J. Using any program/script/command or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet, or initiating any denial of service attacks.
- K. Providing any confidential information about UCLA Healthcare employees to anyone, including other UCLA Healthcare employees, unless the provision of such information is part of the employee's job responsibilities and is authorized by the University policy.
- L. E-Mail and Communication Activities.
 - 1) Sending any electronic communication that does not comply with the "University of California Electronic Communications Policy."
 - 2) Sending any e-mail that contains Protected Health Information (and does not comply with Security Policy No. 9453-A, "*Use of E-Mail in Communication of PHI.*")
 - 3) Sending unsolicited "junk mail" or other advertising material to individuals who did not specifically request such material (e-mail spam).
 - 4) Any form of harassment sent by e-mail, telephone or paging, whether through language, frequency or size of messages.
 - 5) Unauthorized use, or forging of e-mail header information.

- 6) Solicitation of e-mail for any other e-mail address, other than that of the poster's account, with the intent to harass or to collect replies.
- 7) Creating or forwarding "chain letters," "Ponzi" or other "pyramid" schemes of any type.
- 8) Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

M. Unsecured Wireless Communication.

Access to MedNet via unsecured wireless communication mechanisms is prohibited. The requirements set forth in Policy No. 9457 "*Technical Security*" for Wireless Communications shall apply to 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; however, any PHI-containing data streams would still require encryption.

4. Questions

Should an Employee have any question or concern about the appropriate security measures or use requirements, the Employee should first discuss the issue with his or her supervisor. Supervisors should contact the Security Officer at extension 53730 with any questions regarding these security policies and procedures, or by email at HIPAA.Security@mednet.ucla.edu.

APPROVAL

Corporate Compliance Committee

Carole Klove, RN, JD
Chief Compliance and Privacy Officer

REVISION HISTORY

Approved: February 22, 2006
Effective Date: April 20, 2005
Revised: November 2005

REFERENCES

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

California Medical Information Act, California Civil Code Section 56 *et seq.*

University of California Business and Finance Bulletin IS-3, Electronic Information Security

University of California Electronic Communications Policy (ECP)

University of California Los Angeles, Policy No. 420 *'Notification of Breaches of Computerized Personal Information'*

Information Practices Act of 1977, California Civil Code, §§1798.29 and 1798.82.