USE OF ELECTRONIC MAIL (EMAIL) IN COMMUNICATION OF PATIENT IDENTIFIABLE INFORMATION (PROTECTED HEALTH INFORMATION)

PURPOSE

To establish a policy for utilization of email for communicating patient identifiable health information ("PHI") that safeguards confidentiality and meets applicable state and federal laws and regulatory standards.

DEFINITIONS

"Protected health information" or "PHI" is any individually identifiable health information regarding a patient's medical or physical condition or treatment in any form created or collected as a consequence of the provision of health care, in any format including verbal communication.

"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.

POLICY

It is the policy of UCLA Health System to protect the privacy and confidentiality of information when transmitted electronically consistent with federal and state laws and regulations and University policies.

The professional, ethical and legal guidelines and requirements applicable to traditional communications between health care providers and/or their patients also apply to electronic communications.

I. Email Systems

Electronic Protected Health Information (ePHI) should only be transmitted in electronic mail within the UCLA Health System MedNet email system (e.g. with the @mednet.ucla.edu address).

II Minimum Necessary Use of ePHI

UCLA Health System providers and staff are responsible for taking reasonable steps to protect patient privacy and to guard against unauthorized use of PHI. Only the information necessary to accomplish the purpose should be transmitted and should be distributed to only those with a legitimate "need to know". Disclosures of PHI in email should be in

accordance with Privacy Policy No. 9401 "*Protection of Confidential Patient Information (Protected Health Information).*

III. Patient Consent

Prior to the initiation of online communications between a provider and a patient, the patient's prior written consent should be obtained regarding the appropriate use and limitations of this form of communication.

IV. Emergency Subject Matter

Email should never be used for urgent or emergency problems and cases. UCLA Health System providers, staff, and patients should be made aware of the risks associated with online communication related to emergency medical situations by making it clear that email should not be utilized to report or seek advice or treatment for an emergency condition. Patients should be instructed to call their physician directly or 911 for emergency assistance, as appropriate.

V. Authentication

UCLA Health System providers and staff have a responsibility to take reasonable steps to authenticate the identity of correspondent(s) in an electronic communication and to ensure that recipients of information are authorized to receive the communication.

VI. Unauthorized Access

The use of online communications may increase the risk of unauthorized distribution of patient information (but should also create a clear record of this distribution). UCLA Health System providers and staff should establish and follow procedures that help to mitigate this risk. When inappropriate access has occurred, the provider or staff member may have an obligation to inform the patient of that fact. The Privacy Officer should be consulted in all such cases.

PROCEDURES

I. General Guidelines

The following general guidelines shall be followed in transmitting PHI through electronic mail. Additional guidelines, as specified by UCLA Policy 455: UCLA Email Policy and Guidelines, also apply when using email to conduct University business.

A. Sensitive health information such as that dealing with mental health, chemical dependency, sexually transmitted diseases, HIV or other highly personal information should not be transmitted via email. Other, more appropriate venues should be utilized for distributing this information.

B. Each recipient on the distribution list must have an individual email address. Do not send electronic mail containing PHI to a mailing list or to shared email accounts.

C. No PHI should be typed in the "subject field" caption of an email message.

D. The following footer should be included in all emails containing PHI:

"IMPORTANT WARNING: This email (and any attachments) is only intended for the use of the person or entity to which it is addressed and contains information that is privileged and confidential. You, the recipient, are obligated to maintain it in a safe, secure and confidential manner. Unauthorized re-disclosure or failure to maintain confidentiality could subject you to federal and state penalties. If you are not the intended recipient, please immediately notify us by telephone or return email and delete this message from your computer."

E. Except in the case of direct communication with patients, emails with PHI should be sent only to other UCLA Health System mail accounts when conducting UCLA Health System business. Exceptions to this policy must be approved by the Security Officer in consultation with the Department Administrator.

F. Emails sent over the UCLA Health System network are not always protected from interception and may be read at their destination by individuals other than the intended recipient. Encryption should be utilized for all messages when available. If encryption is unavailable, the sender should mask patient identity using medical record number and/or first and last initials or utilize other mechanisms to protect the confidentiality of PHI. UCLA Health System providers and staff should be discreet in their use of email in communicating PHI to colleagues.

II. E-Mail Between Clinician and Clinician

A. A copy of all messages, which are pertinent to a patient's care, should be placed in the patient's medical record.

B. The sender should indicate the category of transaction (e.g., consultation request) in the subject line of the message for purposes of clarification and/or filtering.

C. No person shall make a change to another person's message and pass it on without making it clear where the person has made the changes.

III. E-Mail Between Clinician and Patient

A. Patient Authorization.

The patient must authorize the use of email for communicating patient PHI in writing (*see*: sample Email Consent Form attached as Appendix 1). Patient authorization forms should include the following items:

1. Turnaround time for email messages;
2. Instructions on how to escalate to phone calls and office visits; and
3. Statement indemnifying UCLA Health System for information loss due to technical failures.

The signed authorization must be filed in the patient's medical record.

B. Limit to Administrative Communications and Routine Requests.

The email transmission of PHI should be limited to administrative communications and routine requests for medical information (such as scheduling appointments and refilling prescriptions).

C. Additional Patient Instructions.

Patients should be instructed to put a transaction category (e.g., prescription, appointment, medical advice, etc.) in the subject line of the message for filtering. Patients should also be requested to put their name and patient identification number in the body of the message.

D. Medical Record

All direct email communication with a patient must be considered a part of the medical record. The levels and procedures related to privacy and confidentiality of the traditional paper medical record need to also apply to all email communications.

E. Doctor-Patient Relationship: Licensing Considerations.

Online interactions between a health care provider and his or her patient are part of the doctor-patient relationship. Communications with a patient who resides outside of the State of California may create a risk for those physicians not licensed in that state.

IV. Chief Compliance and Privacy Officer

All instances in which a patient's right to privacy has or may have been compromised via outgoing or incoming emails, should be reported immediately to the UCLA Health System's Chief Compliance and Privacy Officer at 310-825-7135

FORMS

Email Consent and Use Agreement (Patient-Provider) – Appendix 1

REFERENCES

Health Insurance Portability and Accountability Act, 45 CFR 160-164
California Medical Information Act, California Civil Code, Section 56 et seq.

REVISION HISTORY

Create Date: April 2, 2003
Approval Date: April 8, 2003, April 6, 2004, February 22, 2006
Review Date: April 6, 2004, April 8, 2005
Revised Date: April 6, 2004, April 20, 2005, November 2005; June 19, 2007, May 30, 2008

Formerly Policy No.9450 Use of Electronic Mail (email) in Communication of Patient Identifiable Information (PHI)

APPROVAL

HIPAA Committee

HIPAA Committee
Hospital Compliance Committee

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

Ann S. Chang, CISSP
Information Security Officer