Effective Date:	*04/2003*
Approved Date:	*08/2020*
Revised Date:	*08/2020*
Next Review:	*08/2023*
Owner:	*Liangzhou Chen: Mgr*
Policy Area:	*Compliance*
Reference Tags:	*Lippincott*
Applicability:	*Ronald Reagan, Resnick, Santa Monica, Ambulatory Care*

Use of Electronic Mail (Email), HS 9453-A

PURPOSE

The UCLA Health Sciences is committed to safeguarding the confidentiality of patient and other sensitive information transmitted via email consistent with federal and state laws and regulations and University policy.

DEFINITIONS

"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" 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.

"Health Sciences Email Account" means an Information Security and Solutions-supported email account. This includes @mednet.ucla.edu email addresses and others listed in the **Health Sciences Email Standard**.

"University Business" means any activity associated with the performance of one's duties as any employee, trainee, or volunteer, at any time of day or from any location.

"Workforce" means employees, volunteers, and other persons whose conduct, in the performance of their work for UCLA Health Sciences, is under the direct control of UCLA Health Sciences or the Regents of the University of California, whether or not UCLA Health Sciences pays them. The Workforce includes employees, faculty, 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 Health Sciences facilities from another institution.

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 Orthopedic Hospital, the Resnick Neuropsychiatric Hospital at UCLA, the Faculty Practice Group, all ambulatory clinics, the David Geffen School of Medicine, UCLA School of Nursing, UCLA School of Dentistry, and UCLA Fielding School of Public Health (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

In order to provide safeguards for confidentiality of patient and other sensitive information, UCLA Health Sciences use of email is subject to the following:

I. **Workforce members must use Health Sciences Email Accounts for any University Business conducted by email.**
   Only email accounts listed in the **Health Sciences Email Standard** may be used for University Business.

   A. Campus Bruin OnLine email accounts (Gmail through Google Apps for UCLA) may not be used for University Business.

   B. Health Sciences emails may not be auto-forwarded to non-Health Sciences email accounts.

C. Non-Health Sciences emails may be forwarded to Health Sciences email accounts.

II. **All emails containing Restricted Information (RI) that are intended for recipients with non-Health Sciences email addresses must be sent via the secure email portal.**

A. Include **#secure** in the subject line to send the email via the secure email portal. Recipients will be sent an email with a link to the secure email portal where they can pick up the message.

B. Attachments need not be encrypted when sent through the secure email portal.

III. **Data Loss Prevention (DLP)**

UCLA Health Sciences has implemented DLP to use automated rules to check for RI in emails sent to non-Health Science email addresses. DLP identifies emails that are highly likely to contain RI and may forward those emails to the secure portal or take other actions to protect confidential content.

IV. **Only use the Minimum Necessary amount of RI when sending emails.**

A. Only the minimum information necessary to accomplish the business purpose should be transmitted and distributed to only those recipients with a legitimate "need to know".

B. Limit use of RI in the subject line as much as possible.

C. Disclosures of PHI in email should be in accordance with Privacy Policy No. 9401 "*Protection of Patient Information (Protected Health Information).*

V. **Be careful when sending emails that contain RI.**

A. Double check the recipient email addresses to make sure the addresses are correct and all recipients are authorized to receive RI.

B. When replying or forwarding email streams, delete any RI in earlier messages that does not need to be included.

C. Avoid using distribution lists as not everybody on the list may be authorized to receive RI.

D. If an email is accidentally sent to the wrong person, attempt to recall it or ask the recipient to delete before reading it. (Ask your IT support group for instructions on how to recall emails). Report any possible breaches as described in VII below.

VI. **Emailing with patients**

A. The MyUCLAHealth patient portal is the preferred method for messaging with patients on care issues as the communications are sent securely and mechanisms exist to allow more than one person to respond. As not all patients have enrolled in MyUCLAHealth and some patients prefer using email, email may also be used for communications with patients as described in this policy.

B. Workforce members may email patients if all the conditions below are met:

i. The patient requested communication via email or the patient initiated the email exchange; and

ii. no sensitive content is involved (see Part D below); and

iii. the email is sent to the patient via the secure email portal (see Section II above).

C. Providers and staff should ensure patients understand that email should not be used for emergent or urgent issues. Patients should understand the expected response times and call if they do not hear back via email.

D. Sensitive or complicated issues should not be communicated to patients via email. **None** of the following clinical laboratory test results and any other related results shall be conveyed to a patient by email or other electronic means:

i. HIV antibody test

ii. Presence of antigens indicating a hepatitis infection

iii. Drug abuse

iv. Test results related to routinely processed tissues, including skin biopsies, Pap smear tests, products of conception, and bone marrow aspirations for morphological evaluation, if they reveal a malignancy

E. Email message content that affects a patient's care must be documented in the patient's medical record.

F. 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. Communications with a patient who resides outside of the State of California may create a risk for those physicians not licensed in that state.

G. Prior approval from the Office of Compliance Services - Privacy (**CompOffice@mednet.ucla.edu**) must be obtained before emailing patients for any fundraising or marketing purposes. (See: HS Policy No. HS 9470, "*Use of PHI for Marketing Purposes*" and HS Policy No. 9471, "*Use of PHI for Fundraising*.")

H. Prior IRB approval must be obtained before emailing patients for research purposes.

VII. **Health Science Email Standard**
Any additional eligibility or technical requirements of the **Health Sciences Email Standard** must also be followed.

VIII. **Privacy Incident Reporting**
If there is a breach or suspected breach of RI related to email, please report the incident immediately to **CompOffice@mednet.ucla.edu**. The Office of Compliance Services - Privacy team will follow up as necessary. See: HS Policy 9459, "*Privacy and Security Incident Reporting*.")

IX. **Questions**
Any questions on emailing Restricted Information should be referred to the Office of Compliance Services - Privacy and Information Security teams (CompOffice@mednet.ucla.edu).

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

XI. **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. Exceptions may be requested by submitting an exception request form.

REFERENCES

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

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

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

California Health and Safety Code Sections 1280.15, 123148 and 1280.18

California Lanterman-Petris Short Act ("LPS Act")

University of California Electronic Information Security Policy (BFB-IS-3)

University of California Electronic Communications Policy (ECP)

UCLA Policy 455: UCLA Email Policy and Guidelines

CONTACT

Office of Compliance Services - Chief Privacy Officer

Office of Compliance Services - Chief Compliance Security Officer

REVISION HISTORY (PRE-POLICYSTAT)

Approval Date:	April 8, 2003, April 6, 2004, February 22, 2006
Effective Date:	April 14, 2003, October 25, 2017
Revised Date:	April 6, 2004, April 20, 2005, November 2005, June 19, 2007, May 30, 2008, March 31, 2011, November 30, 2017

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

APPROVAL

Health Sciences Enterprise Compliance Oversight Board

Approved 12/11/2010

APPENDIX I - OUTBOUND EMAIL FOOTER

The following footer should be configured to be automatically included in all emails containing Restricted Information sent to non-Mednet email addresses:

"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."

All revision dates: 08/2020, 11/2017, 03/2011, 05/2008, 06/2007, 11/2005, 04/2005, 04/2004

Attachments

No Attachments

Approval Signatures

Step Description	Approver	Date
Administration Approval- President and CEO, UCLA Health	Johnese Spisso: Ceo Med Ctr [JB]	08/2020
Ronald Reagan Medical Staff Executive Committee- Chief of Staff	Carlos Lerner: Assoc Prof Of Clin-Hcomp [JB]	08/2020
Santa Monica Medical Staff Executive Committee- Chief of Staff	Roger Lee: Hs Clin Prof-Hcomp [JB]	08/2020
Resnick Neuropsychiatric Medical Staff Executive Committee- Chief of Staff	Aaron Kaufman: Hs Assoc Clin Prof-Hcomp [JB]	08/2020
Hospital System Policy Committee Chair	Jeffrey Bergen: Mgr [KK]	08/2020
Policy Owner	Liangzhou Chen: Mgr	07/2020