Status **Active** PolicyStat ID **8921299**

UCI Health

Last Approved	12/2020
Last Revised	12/2020
Expires	12/2023
Owner	Valerie Dixon: Chief Compliance & Privacy Officer
Policy Area	Hospital: Privacy & Security

Email and Use of Patient Confidential Information

I. PURPOSE

To establish a policy for utilization of email for communicating protected health information ("PHI") and other confidential individually identifiable information (such as research data) that safeguards confidentiality and meets applicable state and federal laws and regulatory standards.

To establish a policy for e-mail communication between UCI Health providers, patients, payers and other entities.

II. SCOPE

This policy and procedure applies to:

1. All UCI Health Information, in all its forms, regardless of where the information resides, who possesses it, who has authority to create, store, transmit and/or utilize it;
    a. Some examples of document formats include but are not limited to: physical paper, electronic PDF, electronic Word, electronic mail (e-mail), electronic HTML, electronic Text, and electronic PowerPoint etc.
2. All computer and network systems owned and/or administered by UCI Health;
3. All UCI Health business units, this includes, but is not limited to: UCI Health subsidiaries; and
4. All employees, contractors, consultants and vendors doing business with UCI Health including any individuals affiliated with third parties that access UCI Health systems.

III. 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.

"Individually identifiable" means that the 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, or other information that, alone or in combination with other publicly available information, reveals the individual's identity.

"Personal identifier" is a uniquely assigned identifier such as social security number, driver's license number, or financial institution account number, which in combination with the individual's name, can be utilized to commit identity theft.

"Breach" is the unauthorized acquisition, access, use or disclosure of protected health information which compromises the security or privacy of such information. Unauthorized acquisition, access, use or disclosure of encrypted ePHI does not constitute a breach.

"Workforce" means all employees, volunteers, and other persons whose conduct, in the performance of their work for UCI Health, is under the direct or indirect control of UCI Health or the Regents of the University of California. Workforce includes all employees, medical staff, and other health care professionals, agency, temporary, contract, and registry personnel, trainees, house staff, students and interns, regardless of whether they are UC Irvine trainees or rotating through UCI Health facilities from another institution.

IV. POLICY

A. Emails containing PHI can be sent securely within the UCI Health email system without the need for encryption.

B. Emails containing PHI or other confidential information such as account numbers, policy numbers, social security number, and other identifying information sent outside of the UCI Health email system must be encrypted. This includes and is not limited to email addresses such as Gmail, AOL, MSN, Yahoo, and others.

    1. Emails may be encrypted by adding [ucsecure] into the subject line of the email (including the brackets).

C. In the limited situations in which the use of encrypted email impedes a business need of the University, unencrypted email may be sent to a documented Business Associate or external component of the University's single health care component with the approval of the Privacy Officer, Security Officer or Legal Counsel. However other safeguards must be utilized to protect the data such as providing minimal information or de-identified data.

D. Email messages must never contain HIV, mental health, chemical dependency or sexually transmitted diseases or other sensitive information. Other more appropriate venues should be utilized for distributing this information such as mail, telephone, fax or personal delivery of the

information.

E. Credit card numbers should **never** be sent or accepted by email even encrypted email.

F. Only the minimum amount of information should be contained within an email message, and the email message must be distributed to only those with a legitimate work related purpose for receiving the information.

G. All disclosures of PHI in an email message must be only to individuals who are permitted to receive the information under State or federal law, or when the patient to whom the information pertains has authorized the disclosure of the information in writing.

H. The preferred method of communication with patients is to use the MyChart Patient Portal. The patient must consent to the use of the service, and electronic authorization is obtained when the patient registers for MyChart.

I. If a patient initiates a request to contact their provider by email for medical information or to discuss medical information, the patient must sign an Email Consent Form (Attachment A) documenting their understanding of the risks of communicating PHI by email, and designating their choice to communicate by encrypted or unencrypted email.

    1. Requests by patients under the age of 18 to communicate via email should be reviewed by the Compliance & Privacy Office.

J. If a patient initiates a request by email for information that does not contain PHI, such as directions to the medical center or an ambulatory practice, the email request initiated by the patient can be accepted as consent for the specific communication.

K. Email should never be used for urgent or emergency problems and situations to report or seek advice or treatment in an emergency condition. Patients should be instructed to call their physician directly or 911 for emergency assistance as appropriate.

L. Copies of emails between providers and patients must be uploaded into the patient's medical record, either directly by the provider or by submitting a printed copy of the email to Health Information Management.

M. All workforce members must safeguard information sent via email by taking reasonable steps to authenticate the identity of the person(s) to whom the email is being sent is correct, and verifying the email address before sending.

N. Workforce members must immediately notify the Compliance and Privacy office of any emails that were sent to an incorrect email address.

O. The actual or attempted use of another UCI workforce member's email account with or without their permission is prohibited.

P. Incidental personal use of UCI email is permitted; however, the use of UCI email and resources for non-UCI business and excessive personal use is prohibited. Intentional creation and exchange of solicitations, chain letters, or other unofficial email is prohibited.

Q. Auto-forwarding to unapproved third party email services is prohibited. The forwarding of protected information may violate HIPAA or other state or federal privacy laws and regulations.

R. Monitoring: UCI Health utilizes Data Loss Prevention (DLP) software to ensure PHI is sent with the appropriate logging and protection when transmitted outside of the organization UCI Health email system. Electronic surveillance of user activities in the electronic medical record

may be used to monitor compliance with UC Irvine Health privacy policies. The Privacy Office will investigate questionable access.

S. Reporting Concerns: Knowledge of a privacy violation or a potential violation of this policy must be reported by one of the following methods: SQIS (category: confidentiality); UC Irvine Health Compliance & Privacy Office (888-456-7006); Privacy Officer (714-456-3672); University of California toll-free confidential message line (hotline) at 800-403-4744 or www.ucop.edu/uc-whistleblower/.

T. Corrective Actions: Inappropriate access, use, or disclosure, of patient protected health information is a violation of law and UC policy. Violations may result in corrective and/or disciplinary action up to and including termination of employment. Violations of State/Federal privacy regulations can result in privacy breach notifications to government agencies and the impacted consumer(s), fines or imprisonment, or both.

III. PROCEDURE

Responsible Individuals	Procedure
All Workforce members : **General Information**	A. The following general guidelines should be followed in transmitting PHI and other confidential information through electronic mail. Additional guidelines can be found in the UC Irvine Electronic Communications Policy (800-15) and University of California Policy IS-3. 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. Do not forward or send sensitive data to a third party. C. No PHI or other personal identifiers should be typed in the "subject field" caption of an email message. D. The following footer should be included in all emails containing confidential information: *"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."*
Providers (with Other Providers)	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 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.
Providers and Email with Patients	A. The preferred method of communication with patients is to utilize MyChart. The patient will be requested to complete the consent to use the system when they enroll. There is no registration fee for patients. B. If a patient requests to communicate directly with a provider via email, the patient must sign the Email Consent form in order for a UCI Health provider to continue to communicate with the patient via email. (Attachment A: Email Consent Form). C. The patient must be an adult 18 years or older, or the legal representative of the patient. D. The patient must authorize communication to occur via encrypted or unencrypted email. E. No email messages with patients should ever be conducted through a non-UCI email address. F. The email transmission of PHI should be limited to administrative communications and routine requests for medical information (such as scheduling appointments and refilling prescriptions). G. 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 MRN in the body of the record. H. All direct email communication with a patient must be considered a part of the medical record. A copy of the email must be uploaded into the patient chart, either directly by the provider or by submitting a printed copy of the email to Health Information Management. I. Online interactions between a healthcare provider and his or her patient are part of the patient-doctor 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. J. Patient lab results may only be communicated through encrypted email. Additionally, e-mail may not be used for results of testing related to HIV, sexually transmitted

	disease, hepatitis, drug abuse, or presence of malignancy, or for care related to alcohol abuse or mental health.
All workforce members: Misdirected Emails	If a workforce member suspects that a patients' email has been misdirected they must immediately: 1. Complete an incident report regarding the potential privacy breach via the Online Incident Reporting System using the category of confidentiality, OR 2. Contact the UCI Health Compliance & Privacy Office at 714-456-7006 or 1-888-456-7006.

V. REGULATORY

State and federal law require the protection of the confidentiality of health information in any form, including electronic information. Transmission of confidential individually identifiable information via email can pose a risk to the confidentiality of the information as the data passes along computer networks. In addition to the risk of copies of the information sitting on computer network servers, there is a significant risk that the information may be intercepted and accessed by individuals who are not permitted or authorized to receive the information. State law imposes significant penalties and fines on individual staff members and the organization as whole for breaches of patient privacy, including through electronic mechanisms.

The federal HIPAA law also provides patients with a right to receive unencrypted protected health information if they request to receive the PHI in this format.

It is the policy of UCI Health 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.

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 IS-3
University of California Irvine Electronic Communications Policy 800-15

Attachments

Email Consent Form 2021

Approval Signatures

Step Description	Approver	Date
Governing Body	Governing Body [FB]	12/2020
Med Exec Committee	Medical Executive Committee [FB]	12/2020
Policy & Communications Committee	Policy & Communications Cte [JL]	12/2020
Privacy & Security Policy Committee	Compliance & Privacy Office [AR]	12/2020