

**TITLE: COMMUNICATING PROTECTED HEALTH INFORMATION  
VIA ELECTRONIC MAIL (EMAIL) AT COLUMBIA  
UNIVERSITY MEDICAL CENTER**

**POLICY:**

Columbia University Medical Center (CUMC) will permit email of unencrypted Protected Health Information (PHI) under limited circumstances where the appropriate safeguards described herein are applied. CUMC is moving towards requiring encryption for all email of PHI utilizing CUMC electronic mail systems (CUMC email). ***Note: For the purpose of this policy, the term “CUMC electronic mail systems” does not refer to the physical location of the email system but its use by CUMC workforce to transmit PHI.***

**PURPOSE :**

This Policy describes procedures that govern an individual’s use of a CUMC email system. It also defines the steps that must be taken by CUMC patients who wish to engage in email with CUMC. This policy applies to the informational uses of email and does not cover the ethical, legal and regulatory issues associated with email consultations and whether they can be billed to patients.

This Policy applies to CUMC workforce and other persons affiliated with or authorized by CUMC to read, create, store, respond, or transmit information via a CUMC email system (Users). This Policy also applies only to the use of email for both internal and external communications of PHI.

**PROCEDURES:**

**1. Communicating PHI via Email Internally**

- a. As a general rule, unencrypted email should not be used to communicate PHI. Email is inherently less secure than other forms of communication. However, email of PHI will be permitted at CUMC if certain safeguards are implemented.
- b. CUMC will implement the following safeguards when communicating PHI in or attached to an email message:
  - (1) Email communications containing PHI about CUMC patients will be transmitted only on a CUMC or NYPH email system and ***cannot be forwarded to an email account outside CUMC or NYPH.***
  - (2) PHI will not be transmitted in the subject line of the email message.
  - (3) The fact that the message or an attachment to the message contains PHI will be reflected in the subject line of the email message.
  - (4) The email message will include the following confidentiality notice:  
***“This electronic message is intended to be for the use only of the named recipient, and may contain information that is confidential or privileged. If you are not the intended recipient, you are hereby***

*notified that any disclosure, copying, distribution or use of the contents of this message is strictly prohibited. If you have received this message in error or are not the named recipient, please notify us immediately by contacting the sender at the electronic mail address noted above, and delete and destroy all copies of this message. Thank you.”*

Note: This confidentiality notice can be added to the signature block of your email signature if you currently use an automated signature.

- (5) PHI that is specially protected (i.e., HIV/AIDS information, substance abuse treatment information, and mental health information) will not be communicated via email.
  - (6) If a document that contains PHI is attached to the message, the User should verify before transmitting the email message that he/she has attached the proper attachment.
  - (7) Before transmitting the email message, Users should double-check the message and any attachments to verify that no unintended information is included.
  - (8) Users who communicate PHI via email will comply with all other CUMC policies and procedures including, but not limited to, the Confidentiality of PHI Policy and the Minimum Necessary Policy.
- c. Any User who is unsure whether an email message or attachment contains PHI should contact his/her supervisor or the HIPAA Privacy Officer before initiating the email communication.

## 2. Communicating PHI with Patients

- a. Patients have the right to request that CUMC communicate with them via email.
- b. If a patient requests email communications containing their PHI, the individual receiving the request must obtain a completed **Request for Email Communications** form from the patient AND must provide the patient with the **Important Information about Provider/Patient Email** form prior to processing the patient's request.

Both forms are available on the CUMC website. Click on Administrative Services or Patient Care from the home page, then click on the link to HIPAA on the right side of the page. Select the forms needed from the list of forms available on the left side of the page.

- c. CUMC reserves the right to deny a patient's request to communicate with him/her via email. For example, a patient's request for email communications may be denied by CUMC if a provider with an existing clinical relationship with the patient believes email communications with the patient should not occur.

- d. If the patient's initial request to communicate via email is granted by CUMC, the patient will be required to complete the following prior to engaging, for the first time, in provider/patient emails with CUMC:
  - (1) Respond to a test email with answers to a question specific to that patient (i.e., the patient's date of birth, father's name, mother's name, etc.) to verify the patient's email address and identity; and
  - (2) Read and understand the Important Information about Provider/Patient Email form confirming the patient's understanding of the risks of engaging in email communications with his/her providers.
- e. No specially protected PHI (i.e., HIV/AIDS information, substance abuse treatment information, and mental health information) will be communicated via email even if the patient's request for email communications is granted.
- f. All completed Request for Email Communications forms will be maintained by the office processing the patient's request for a minimum of six (6) years. Approved requests are valid regardless of the time period as long as a hard copy of the form is maintained.
- g. An approved Request will be effective for only the health care provider identified on the Request. The patient must complete a separate Request for each health care provider with whom he/she wants to communicate via email, and must revoke each Request to discontinue email communications.

### **3. Ownership of Electronic Mail**

- a. The email systems at CUMC belong to Columbia University.
- b. CUMC workforce will adhere to this policy when sending PHI and Columbia University's email policy when sending email that doesn't contain PHI.
- c. CUMC reserves the right to override individual passwords and access the email system at any time for valid business purposes such as system maintenance and repair and security investigations.

### **4. Retention of Email**

- a. CUMC regularly archives email for the purposes of record recovery and regulatory compliance.
- b. Questions about retention activities should be directed to the Information Security Officer.

### **5. Definitions**

*User* means any employee or other person authorized by CUMC to read, enter or update information created or transmitted via the electronic mail system.

*Protected Health Information (PHI)* means information, including demographic information that may identify the patient, that relates to the past, present or future physical or mental health or condition of an individual, the provision of health care to an individual or the past, present or future payment

for the provision of health care to an individual and identifies or could reasonably be used to identify the individual.

*Workforce* means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for CUMC, is under the direct control of CUMC, whether or not they are paid by CUMC.

**APPLICABILITY**

**CUMC WORKFORCE**

**RESPONSIBILITY:**

HIPAA Privacy Officer, Information Security Officer, Vice Presidents

**REVIEW/REVISION DATE:**

January 21, 2004