Email Usage Policy

Provides guidance for: proper use of email, necessary actions for sending sensitive data via email and privacy expectation

Overview

I. Introduction

Email is an expedient communication vehicle to send messages to the Columbia University community. The University recognizes and has established the use of email as an official means of communication. However, use of an email system at the University requires adequate security measures to protect the University Data (as such term is defined in the Columbia University Information Security Charter (the "Charter")) that is transmitted.

Capitalized terms used herein without definition are defined in the Charter.

II. Policy History

The effective date of this Policy is November 1, 2013. This Policy and other Information Security Policies replace (A) the following University Policies:

- Electronic Information Resources Security Policy, dated March 1, 2007
- Email Usage and Retention Policy, dated April 1, 2008

and (B) the following CUIMC Policy:

- Communicating Protected Health Information via Electronic Mail (Email) at Columbia University Medical Center, dated January 21, 2004, and amended as of September 21, 2012

Policy Text

III. Policy Text

A. Approved University Email Systems

All email used to conduct University business must be transmitted via an Approved University Email System. For purposes of this Policy, an "Approved University Email System" is Lionmail, any CUIT or CUIMC IT Email System and any other Email System that has been risk assessed and approved by the applicable Information Security Office.

B. Prohibited Actions

No User of University email may take any of the following actions:

1. Send or forward an email through a University System or Network for any purpose if such email transmission violates laws, regulations or University policies and procedures;
2. Use any Email System other than an Approved University Email System to conduct University business or to represent oneself or one's business on behalf of the University. Examples of Email Systems that are not approved include a personal email account or a personal Columbia Alumni Association account (i.e., anything@caa.columbia.edu).
3. Send nuisance email or other online messages such as chain letters;
4. Send obscene or harassing messages;
5. Send unsolicited email messages to a large number of Users unless explicitly approved by the appropriate University authority; or
6. Impersonate any other person or group by modifying email header information to deceive recipients.

C. Provisions Relating to Emails Containing Sensitive Data

Each User shall ensure that Sensitive Data is transmitted by email only if the following conditions are met:

1. Except as provided in Section D below, all email communications of Sensitive Data are encrypted before being transmitted.
2. Sensitive Data are not transmitted in the "Subject" line of an email.
3. Before transmitting an email that contains Sensitive Data, the User verifies that no unintended information is included in the message or any attachment and that the proper document is attached.
4. Before transmitting an email that contains Sensitive Data, the User verifies the names and email addresses of the intended recipients.

D. Provisions Relating to Email Within the Columbia Health Care Component

For purposes of this Policy, an "Approved OHCA Email System" is any CUIT Email System other than Lionmail, any CUIMC IT Email System and any other Email System used within the CUIMC/Hospital OHCA that has been approved by the CUIMC Information Security Office.

The following provisions relate only to email transmitted by Users within the Columbia Health Care Component:

1. Unencrypted EPHI may be transmitted internally if sent on an Approved OHCA Email System.

2. No automatic forwarding, redirection or automated delivery of email outside the CUIMC/Hospital OHCA may be used.

3. Email messages containing EPHI must include a confidentiality notice substantially in the form of the following text:

“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 email address noted above, and delete and destroy all copies of this message. Thank you.”

4. Any User who requires guidance in determining whether an email message or attachment contains Sensitive Data must contact his/her supervisor or the Office of HIPAA Compliance before initiating the email communication.

E. Communicating PHI to Patients via Email

1. Patients have the right to request that Users within the Columbia Health Care Component communicate with them via email.
2. Subject to Section 3, all email communications with patients must be transmitted in encrypted form on an Approved University Email System. The subject line of the email communication must include #encrypt and must not include any PHI.
3. At the request of a patient, email communications may be sent in unencrypted form, provided that the patient completes the appropriate email authorization form and submits it to the Office of HIPAA Compliance or the patient’s health care provider has submitted the patient’s request prior to sending the first unencrypted communication to the patient.
4. The University 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 the University if a health care provider with an existing clinical relationship with the patient does not agree that email communications should be used with the patient.
5. Patients should be encouraged to use their electronic personal health record to communicate with their health care providers.

F. Privacy Expectations

The University observes the Privacy Expectations described in the Columbia University Acceptable Usage of Information Resources Policy with respect to email.

For reasons relating to compliance, security or legal proceedings (e.g., subpoenas) or in an emergency or in exceptional circumstances, the Office of the General Counsel may authorize the reading, blocking or deletion of University Data. In particular, in the context of a litigation or an investigation, it may be necessary to access University Data with potentially relevant information. Any such action taken must be immediately reported to the Office of the General Counsel and the applicable Information Security Office.

The University may record information about certain data elements of email messages in the course of monitoring or maintaining its email systems. These data include, but are not limited to: (a) the identity and address of the authenticated sender, (b) the address of the recipient, (c) the size of the message, (d) the transmission time, (e) the headers of the email, (f) the subject of the message, (g) the number of attachments and (h) certain features that are used to identify spam.

CUIMC uses a Data Loss Prevention (DLP) solution that filters outbound email messages and attachments to identify the presence of character patterns resembling Sensitive Data, examples of which could include social security numbers, credit card numbers, patient record numbers or certain identifiable data elements that constitute EPHI. Upon detecting a character pattern that might reflect the presence of Sensitive Data, the DLP appliance blocks the email and automatically sends a message to the sender instructing him/her to re-send the contents in encrypted form or to take comparable appropriate action. The filtering consists of automatic scanning for prescribed character patterns and does not permit reading the contents of the email.

IV. Cross References to Related Policies

The Information Security Policies referred to in this Policy are listed in Appendix A hereto.

Cross Reference(s) to Related Policies

Related Policies

Acceptable Usage of Information Resources Policy

Information Security Charter

Effective Date

Published: October 2013

Revised: November 2014, April 2016, July 2019

✉ cuit-risk@columbia.edu

Responsible University Office

Information Technology (CUIT)

Audience

Officers of Administration
Students
Visitors and Consultants
Researchers
Faculty
Support Staff (Non-Union)

Support Staff (Union)

Librarians

Category

Annual Notice