Weill Cornell Medicine

11.08

Use of Email

Responsible Executive: Chief Information Officer, WCM
Original Issued: December 15, 2010
Last Updated: May 20, 2016

Policy Statement

Weill Cornell Medicine (WCM) provides a centrally-managed email service to faculty, staff, students, and affiliates for the purpose of furthering the mission of education, research, and patient care and for conducting general college business. While incidental and occasional personal use of email is permissible, personal communications and data transmitted or stored on WCM information technology resources (such as email) are treated as business communications, and are subject to automated surveillance by security systems managed by the Information Technologies & Services (ITS) Department.

Reason for Policy

WCM is legally responsible to protect confidential information, including that contained in email. WCM and NYP email systems comply with appropriate security standards. Because WCM cannot guarantee the security of external systems, WCM has chosen to prohibit the use of automated email forwarding and requires encryption for any email message containing confidential information that is sent outside the WCM/NYP network.

Entities Affected by this Policy

Weill Cornell Medicine

Who Should Read this Policy

All individuals with a Weill Cornell Medicine email account sending and receiving email pertaining to Weill Cornell Medicine and/or an affiliate organization.

Web Address of this Policy

https://its.weill.cornell.edu/policies/

Contacts

Direct any questions about this policy, 11.08 – Use of Email, to Brian J. Tschinkel, Information Security Officer, using one of the methods below:

- Office: (646) 962-2768
- Email: brt2008@med.cornell.edu

Contents

1. Principles

Certain information such as protected health information (PHI), personally identifiable information (PII), or financial records are confidential and must be treated with extreme care to avoid inappropriate disclosure that could lead to exposure of risk to Weill Cornell Medicine and its affiliates. A complete list of all data considered confidential by WCM is available in the ITS 11.03 – Data Classification policy.

While the college permits generally unhindered use of its information technology resources, those who use WCM information technology resources do not acquire, and should not expect, a right of privacy. WCM community members should not expect that personal communications will remain private and/or confidential. Automated email surveillance systems are in place to identify data that appear malicious in nature (e.g., viruses, spyware) or contain confidential information (e.g., protected health information and personally identifiable information) for further investigation.

2. Email Account Owner Responsibility

WCM provides a centrally-managed email system for its faculty, staff, students, and affiliates. No additional email systems are permitted without approval of the Chief Information Officer. WCM-supplied email accounts (@med.cornell.edu) are unique and assigned to an individual for communication pertaining to WCM. Except in cases approved by WCM Human Resources or General Counsel, these email accounts are not transferrable to other users. Access to WCM's email system requires certain responsibilities for the account holder, including, but not limited to, the following:

- Do not share your email account password with anyone, including ITS (ITS will never ask you for your password). Use delegation, where appropriate, if another user needs access to your email.
- Do not use email to harass others.
- Do not falsify email accounts to send out email as another person.
- Do not flood/spam people with email in an attempt to disrupt their service.
- Do not accept credit card numbers sent in email for payment purposes.
- Do not create rules that enable automated forwarding to non-WCM email accounts.
- Do not send confidential data to any party via email without using encryption.
- Do not use personal email addresses, such as Gmail or Yahoo!, for work-related communications.

3. Public Display of Email Addresses

As defined in the ITS 11.03 – Data Classification Policy, WCM email addresses are not considered confidential data. In the interest of transparency, all active Weill Cornell Medicine faculty and staff email addresses (including physicians and other providers) are published on the College's website, directory, and VIVO. WCM email addresses themselves are not confidential information (please see ITS 11.13 – Directory). A patient's email address is considered an identifier that could link to protected health information under HIPAA.

Physicians who receive emails from patient should ensure all communications are delivered through secure means, as described in this policy. Physicians who do not wish to communicate with patients should instruct their patients to utilize the Weill Cornell CONNECT platform.

4. Email Attachment Policy

In order to align WCM with generally accepted email standards, ITS limits the size of all outgoing and incoming email messages, including attachments, to 25 megabytes (MB). Many email systems cannot receive large emails and often do not provide feedback to the sender that the system has rejected the message. By aligning with the industry common

practice of limiting email sizes, users should have a higher success rate in sending and receiving email. If attachments larger than 25 MB need to be sent via email, WCM's File Transfer Service should be used.

5. Transmission of Confidential Data

Any data considered by WCM to be confidential in nature that must be transmitted via email shall utilize encryption when sent over an insecure network and shall only be sent to recipients that have a legitimate need for the information.

5.01 Internal Recipients (WCM, NYP, and Select Affiliates)

Email sent within WCM's network is considered to be contained within a trusted secure environment. WCM's network includes addresses ending in @med.cornell.edu, @nyp.org, @mskcc.org, @rockefeller.edu, @hss.edu. While an explicit encryption service is not required for data sent to these recipients, it is still strongly recommended to utilize WCM's File Transfer Service when sending large attachments containing confidential data.

5.02 External Recipients

Email containing confidential data that is sent outside of WCM's network (as defined in the previous section) must use encryption. Email messages smaller than 25 MB may be sent securely by adding #encrypt to the message subject. When using #encrypt, both the message body and attachments are encrypted. To securely send large attachments to external recipients, WCM's File Transfer Service shall be used; however, only the attachments will be encrypted and no confidential data is to be referenced within the subject or body of the message.

5.03 Routine Communication with External Agencies

For routine communication with external agencies (e.g., a business associate like a pharmaceutical company or a collection agency), ITS can assist in establishing an encrypted channel by enforcing Transport Layer Security (TLS), a popular encryption protocol for securing data in transit. WCM utilizes opportunistic TLS to first attempt to negotiate a secure and encrypted connection with an outside domain. In the event the recipient domain does not support TLS, the connection will not be encrypted but messages will be sent. By choosing to force TLS, ITS will work with the external vendor to always force encryption between WCM and the recipient domain. While this will guarantee a secure delivery, any anomalies or inaccuracies in the domain or a rejection by the recipient mail system will prevent messages from being sent altogether.

For entities performing services or functions on behalf of WCM (e.g., a transcriptionist, answering service, etc.) that involve the exchange of confidential data, a Business Associate Agreement (BAA) shall be on file with the WCM Privacy Office and encryption must be used to safeguard the message contents.

A list of external agencies with an established encrypted channel is maintained on the ITS website.

5.04 Communication with Patients

WCM community members wishing to communicate electronically with patients may do so using the Weill Cornell CONNECT service. It is strongly discouraged to communicate with patients via email. However, if a patient insists on email communication, encrypted email services must be used. Recipients must be cautioned to only reply within the secure mail console as replying to the notification (or otherwise outside the console) will result in the message being sent without encryption.

5.05 Email Confidentiality Notice

Individuals transmitting confidential or high risk data may add a confidentiality notice to the footer of their email in order to notify the recipient of the sensitivity of the data contained within the message. The following language is recommended for use in an email signature:

> *Confidentiality Notice: This email transmission, and any documents, files, or previous email messages attached to it, may contain confidential and/or privileged information and may be legally protected from disclosure. Any unauthorized review, use, disclosure, or distribution is strictly prohibited. If you are not the intended recipient, or a person*

responsible for delivering it to the intended recipient, please contact the sender by reply email and destroy all copies of the original message, including any attachments.

6. Email Forwarding

Automated email forwarding for active WCM faculty members is permissible under certain circumstances to qualified affiliate domains. Any requests to allow forwarding must be approved by WCM Human Resources, General Counsel, or the Office of Faculty Affairs. **WCM faculty, students and staff are not permitted to forward email once in expiry status.**

7. Email Account Delegation

Delegation occurs when an email account owner (the "delegator") grants permissions to another user ("the delegate") to access the owner's email, calendar, and/or contacts. Delegation is not permitted by sharing passwords or logging in to the account for the delegate to use – the delegate must be using his/her own account. Delegators have the ability to set variable permissions to the delegate, such that the delegate has the ability to only read emails or also create emails on behalf of the delegator.

Delegation is only to be used in situations where an assistant or coworker needs access to a mailbox account that are in the confines of the delegate's job responsibilities. The delegator is responsible for ensuring that the delegate's permissions are appropriate and consistent with his/her job description and training.

8. Email Account Retention

Once in expiry status, certain provisions apply in order to retain a WCM email account. Faculty, staff, and students on a leave of absence are permitted to retain their WCM email account. Any exceptions to the following provisions must be approved by WCM Human Resources, General Counsel, or Office of Faculty Affairs.

8.01 Students

Students who graduate from WCM and do not continue an affiliation with WCM are not permitted to retain full access to their WCM-issued email account. Instead, alumni may request to receive an alumni email mailbox (e.g., CWID@alumni.weill.cornell.edu). Alumni mailboxes are equipped with anti-spam and anti-virus protection, multifactor authentication, and security reminders when attempting to send confidential data. The Graduate School and Office of External Affairs will coordinate the offboarding process when students are nearing graduation. The ITS data loss prevention tool is in place to monitor and block email potentially containing confidential data that is sent to alumni addresses. WCM alumni who become residents at NYP will be provided with an NYP email account in addition to retaining the WCM alumni mailbox.

8.02 Faculty

At the discretion of a Department Administrator, Chairperson, Director, or the Office of Faculty Affairs, WCM faculty may be permitted to retain their WCM-provided email account for three (3) months while in expiry status. Any requests longer than three (3) months will need to be resubmitted and recertified.

Faculty transitioning from WCM to NYP may be permitted to retrieve an export of their @med.cornell.edu mailbox at the discretion of the WCM Department Administrator, Chairperson, or Director. The mail file may need to be scanned for confidential data with the ITS data loss prevention tool. Please note, the @med.cornell.edu address must be deactivated in order to provision an @nyp.org email address. A forwarder is permitted for the existing WCM address to the newly provisioned NYP address only if/while the faculty maintains an active appointment or affiliation with WCM.

8.03 Staff

Unless approved temporarily in exceptional circumstances by the Department Administrator and Human Resources or General Counsel, WCM staff will immediately lose access to their email account once in expiry status. Staff who transition from WCM to NYP are permitted to maintain an email forwarder temporarily in exceptional circumstances.

9. Procedures

9.01 Encrypted Email Services

To send an encrypted message to an external recipient (addresses that do not end in @med.cornell.edu, @nyp.org, @mskcc.org, @rockefeller.edu, @hss.edu), **#encrypt** can be added anywhere in the subject line. The entire message and any attachments will be encrypted and securely delivered to the recipient.

To send large attachments to internal and external recipients, WCM's File Transfer Service should be used. The File Transfer Service can be accessed at **https://transfer.med.cornell.edu**. When utilizing this service, only attachments will be encrypted; therefore, no confidential data shall be disclosed within the body of the message.

Additional Information and User Guides:

- Encrypted Email
- WCM File Transfer Service

To request persistent encryption for routine email correspondence with an outside entity, a support request should be submitted to ITS. Requests must include an adequate business justification and a list of the recipient email domain(s). A Business Associate Agreement should be on file with the WCM Privacy Office.

9.02 Email Forwarding

Active WCM faculty who wish to have their email forwarded to another account must submit a request to ITS support. The request should contain the desired forwarding account, a valid business justification, and the length of time the email should be forwarded. The request will be submitted to Human Resources or General Counsel for approval.

9.03 Email Account Retention

A Department Administrator, Chairperson, or Director wishing to permit a WCM faculty member in expiry status to retain his/her email account must submit a request to ITS support. The request should contain the Department Administrator, Chairperson, or Director's approval and a valid business justification. Forwarding rules will expire after three (3) months and must be resubmitted for approval for any extensions. The WCM faculty member is not permitted to forward email to another account when in expiry status.

A WCM faculty member transitioning to NYP may request to retrieve an export of his/her @med.cornell.edu email account by submitting an ITS Support ticket. The request will need to be accompanied by approval from the WCM Department Administrator, Chairperson, or Director and submitted to ITS Support for processing.

10. Related Documents

The following documents are also relevant to this policy:

- 11.03 – Data Classification
- 11.09 – Data Loss Prevention
- 11.13 – Directory
- 11.14 – Email Security

11. Definitions

These definitions apply to institutions and regulations as they are used in this policy. Definitions of technical terms are supplied by NIST IR 7298 Revision 2, *Glossary of Key Information Security Terms*.

- WCM Weill Cornell Medicine

- ITS — Information Technologies & Services Department
- NYP — NewYork-Presbyterian Hospital
- BAA — Business Associate Agreement
- PII — Personally identifiable information, as defined in GAO-08-536 Privacy Protection Alternatives, is any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.
- PHI — Protected health information, as defined in Title 45 CFR §160.103, is individually identifiable health information that is (i) transmitted by electronic media; (ii) maintained in electronic media; or (iii) transmitted or maintained in any other form or medium. Protected health information excludes individually identifiable health information (i) in education records covered by the Family Educational Rights and Privacy Act (FERPA), as amended, 20 U.S.C. 1232g; (ii) in records described at 20 U.S.C. 1232g(a)(4)(B)(iv); (iii) in employment records held by a covered entity in its role as employer; and (iv) regarding a person who has been deceased for more than 50 years.
- confidential — As defined in ITS 11.03 – Data Classification, confidential data includes, without limitation, the following: PHI; PII; financial data, including data covered under the Gramm-Leach-Bliley Act (GLBA) and the information pertaining to credit cards covered by the Payment Card Industry Data Security Standard (PCI DSS); employment records, including pay, benefits, personnel evaluations, and other staff records; research data involving human subjects that are subject to the Federal Policy for the Protection of Human Subjects (Common Rule) as defined in Title 45 CFR §46.101 et seq.; and user account or system passwords that provide access to information systems or applications containing any of the above confidential data elements.
- expiry — Expiry is used to classify faculty, staff, voluntary, consultants, temps, or students that leave Weill Cornell Medicine. An expiry may occur in any of the following scenarios: resignation, retirement, graduation, layoff, discharge, abandonment of job, cessation of faculty appointments, or expiration of a contracted or otherwise temporary affiliation.