Weill Cornell Medicine	**Policy Title**	Use of Email
	Policy Number	500.08
	Department	ITS Security
	Effective Date	December 15, 2010
	Last Reviewed	July 23, 2024
	Approved By	Tom Horton
	Approval Date	July 23, 2024

Policy

Weill Cornell Medicine 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. As defined in ITS policies 500.01 – Response Use of Information Technology Resources and 500.02 – Privacy of the Weill Cornell Medicine Network and Systems, incidental and occasional personal use of email is permissible. However, personal communications and data transmitted or stored on Weill Cornell Medicine information technology resources (such as email) are treated as business communications and data. Use of a Weill Cornell Medicine email account is subject to monitoring for performance and compliance purposes.

Purpose

Weill Cornell Medicine is legally responsible to protect institutional data, including that contained in email. Weill Cornell Medicine's email system complies with appropriate security standards. Because Weill Cornell Medicine cannot guarantee the security of external systems, Weill Cornell Medicine has chosen to prohibit the use of automated email forwarding and requires encryption for any email message containing High Risk data that is sent outside the Weill Cornell Medicine affiliate network.

Scope

Applies to all members of the Weill Cornell Medicine community who utilize Weill Cornell Medicine information technology resources. This includes Weill Cornell Medicine-Qatar and those responsible for managing and safeguarding Weill Cornell Medicine data.

1. Procedure

High Risk data at Weill Cornell Medicine must be treated with extreme care to avoid inappropriate loss or disclosure that could lead to exposure of risk to Weill Cornell Medicine and its affiliates. A complete list of all data considered high risk by Weill Cornell Medicine is available in ITS policy 500.03 – Data Classification.

Weill Cornell Medicine community members should not expect that personal communications will remain private and/or confidential. Automated email monitoring systems are in place to identify data that appear suspicious or malicious in nature (e.g., viruses, spyware) or contain high risk data (e.g., protected health information and personally identifiable information) for further investigation.

2. Email Account Owner Responsibility

Weill Cornell Medicine provides a centrally-managed email system for its faculty, staff, students, and affiliates. No additional email systems are permitted for business use without the approval of the Chief Information Officer. Email accounts are uniquely assigned to an individual for communication pertaining to Weill Cornell Medicine. Except in cases approved by Human Resources or the Office of General Counsel, these email accounts are not transferable to other users. Access to Weill Cornell Medicine'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 email accounts not affiliated with Weill Cornell Medicine
- Do not send high risk 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 ITS policy 500.03 – Data Classification, Weill Cornell Medicine email addresses are not considered high risk data. In the interest of transparency, email addresses are published on Weill Cornell Medicine's websites, including the Directory and VIVO. Individuals may elect to reduce the visibility of their Weill Cornell Medicine email address as defined in ITS policy 11.13 – Directory.

Clinicians who receive emails from patients should ensure all communications are delivered through secure means as described in this policy. Clinicians who do not wish to communicate with patients should instruct their patients to utilize the Connect patient portal.

4. Email Attachment Policy

In order to align Weill Cornell Medicine 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's 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, the Secure File Transfer Service should be used.

5. Transmission of High Risk Data

Email alone is not generally considered a trusted mechanism for transmitting sensitive data, including data that is classified as High Risk by Weill Cornell Medicine. Email owners should refrain from sending high risk data over email, even among internal recipients, especially if contained in attachments such as spreadsheets or presentations. In the event that email must be used to exchange High Risk data, an ITS-approved encryption solution shall be used, and the recipients shall have a legitimate and authorized need to receive the information.

Individuals shall use the Secure File Transfer Service for sending High Risk data with large file attachments or add **#encrypt** to the message subject for emails with no or small attachments. These services provide an audit trail and adequate security protections for transmitting high risk data. For routine communication with external agencies, including business associates as defined under HIPAA, ITS can assist in establishing an encrypted channel by enforcing Transport Layer Security (TLS) between the parties.

5.01 Communication with Patients

Weill Cornell Medicine community members wishing to communicate electronically with patients shall do so using Connect, the patient portal. It is very strongly discouraged to communicate with patients via email. However, if a patient insists on email communication, encrypted email services shall 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 and is a violation of this policy.

5.02 Email Confidentiality Notice

Individuals transmitting 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 approved and available 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 is permissible under certain circumstances to qualified affiliate domains, typically in cases where an active Weill Cornell Medicine community member is appointed by or an employee of another affiliated institution.

7. Email Account Delegation

Delegation occurs when an email account owner (the "delegator") grants permissions to another individual ("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 their 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 an email account that is 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 their job description and training.

If an email account is intended to be shared by multiple individuals, a shared mailbox shall be used instead.

8. Email Account Retention

Once an individual's affiliation with Weill Cornell Medicine ends, certain provisions apply in order to retain a Weill Cornell Medicine email account. Faculty, staff, and students on a leave of absence are permitted to retain access to their Weill Cornell Medicine email account. Any exceptions to the following provisions must be approved by Human Resources, the Office of General Counsel, or the Office of Faculty Affairs.

8.01 Students

Students who graduate from Weill Cornell Medicine and do not otherwise continue an affiliation with Weill Cornell Medicine are not permitted to retain access to their email account. Instead, as alumni, they may elect to obtain an alumni email account (@alumni.weill.cornell.edu). Alumni email accounts are equipped with anti-spam and anti-virus protection, multifactor authentication, and security reminders when attempting to send high risk data. The 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 high risk data that is sent to alumni email addresses. Alumni who become residents at New York-Presbyterian will be provided with an email account from New York-Presbyterian in addition to retaining their Weill Cornell Medicine alumni account.

8.02 Faculty

At the discretion of a department head, chairperson, or Human Resources, or Office of General Counsel, Weill Cornell Medicine faculty may be permitted to retain their email account for a temporary period after leaving Weill Cornell Medicine. The period will be defined by the approving body.

Faculty transitioning to emeritus status may elect to obtain an emeriti email account (@lifelong.weill.cornell.edu). Emeriti email accounts are available upon approval from the department head or Human Resources.

Generally, email may not be exported from the Weill Cornell Medicine email account. Under extenuating circumstances, an email export file may be created with approval from Human Resources or the Office of General Counsel. The email file may need to be scanned for High Risk data with the ITS data loss prevention tool.

8.03 Staff

Unless approved temporarily in exceptional circumstances by the department administrator and Human Resources or Office of General Counsel, staff will immediately lose access to their email account once their affiliation with Weill Cornell Medicine ends. Staff who transition from Weill Cornell Medicine to New York-Presbyterian may be permitted to maintain an email forwarder temporarily in exceptional circumstances.

Compliance with this Policy

All WCM Workforce Members are responsible for adhering to this policy. Failure to comply will be evaluated on a case-by-case basis and could lead to corrective action, up to and including termination, consistent with other relevant WCM and University Policies. Instances of non-compliance that potentially involve a lapse of professionalism may lead to engagement of the Office of Professionalism for evaluation and intervention.

Contact Information

Direct any questions about this policy, 500.08– [Use of Email], to the Chief Information Security Officer, using one of the methods below:

- Office: (646) 962-3609
- Email: ciso@med.cornell.edu

Policy Approval

Version History

Date	Author	Revisions
December 15, 2010		Initial draft completed
December 9, 2014	Brian J. Tschinkel	Added transmission requirements for high risk data and delegation responsibilities
January 16, 2015	Brian J. Tschinkel	Requires CIO approval for new email systems for business purposes
September 17, 2015	Brian J. Tschinkel	Added provisions for email account retention
May 13, 2023	Brian J. Tschinkel	Updated policy template and language; removed redundant sections
July 3, 2024	Tom Horton	Updated contact information and language
July 12, 2024	Christine Klucznik	Updated policy template and language