	WCM Administrative Policy and Procedure	
Weill Cornell Medicine	**Policy Title**	Use of Email
	Policy Number	ITS-500.08
	Department/Office	ITS Security
	Effective Date	December 15, 2010
	Last Reviewed	July 12, 2024
	Approved By	WCM-Executive Policy Review Group
	Approval Date	June 16, 2026

Purpose

Weill Cornell Medicine (WCM) provides a centrally-managed email service to Workforce Members 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 WCM information technology resources (such as email) are treated as business communications and data. Use of a WCM email account is subject to monitoring and review for performance, legal, and compliance purposes.

Scope

This policy applies to all WCM Workforce Members who utilize WCM Information Technology Resources as well as those responsible for managing and safeguarding WCM data.

Policy

WCM is legally responsible to protect institutional data, including that contained in email. WCM's email system complies with appropriate security standards. As WCM cannot guarantee the security or compliance of external systems, WCM 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 WCM affiliate network.

Definitions

Workforce Members: Faculty; Non-Faculty Academics; Staff; Students; Volunteers; and other persons whose conduct, in the performance of work for WCM, is under the direction and control of WCM, whether or not they are paid by WCM.

Procedure

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

WCM community members should not expect that personal communications will remain private and/or confidential. Email monitoring processes 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.

1. Email Account Owner Responsibility

WCM provides a centrally-managed email system for its Workforce Members. No additional email systems, including non-approved AI email assistants, 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 WCM. Except in cases approved by Human Resources or the Office of General Counsel, these email accounts are not transferable 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 email accounts not affiliated with WCM
- 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.

2. Public Display of Email Addresses

As defined in ITS policy 500.03 – *Data Classification*, WCM email addresses are not considered High Risk Data. While WCM email addresses are published on the Directory and VIVO for transparency, EA-120.01 - *Personal Faculty Websites* prohibits their inclusion on personal faculty websites. Individuals may also elect to reduce the visibility of their WCM email address as defined in ITS policy 500.13 – *Directory*.

3. 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). If attachments larger than 25 MB need to be sent via email, the Secure File Transfer Service should be used.

4. 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 WCM. High Risk Data should not be sent via email unless it is encrypted, 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 or otherwise appropriate encryption solution shall be used, and the recipients shall have a legitimate and authorized need to receive the information. Refer to the ITS Encrypted Email and How to Encrypt Your Email pages for additional details, including supported methods, domains that may automatically be encrypted, and step-by-step instructions for applying encryption to emails containing High Risk Data.

Individuals shall use the Secure File Transfer Service for sending High Risk Data with large file attachments, add **#encrypt** to the message subject for emails with no or small attachments, or use the encryption button provided in the ITS-supported email system. 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.

4.01 Communication with Patients

Clinicians shall direct patients to use the **Connect patient portal** as the preferred and primary method of communication. When patients elect to communicate by email, clinicians must ensure that all correspondence is conducted using approved encrypted email methods in accordance with this policy. Clinicians should continue to encourage patients to transition future communications to the Connect patient portal whenever feasible.

4.02 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.*

5. Email Forwarding

Automated email forwarding is permissible under certain circumstances to qualified affiliate domains, typically in cases where an active WCM community member is appointed by or an employee of another affiliated institution.

6. 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.

7. Email Account Retention

Once an individual’s affiliation with WCM ends, certain provisions apply in order to retain a WCM email account. Workforce Members on a leave of absence are permitted to retain access to their WCM 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.

7.01 Students

Students who graduate from WCM and do not otherwise continue an affiliation with WCM 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 (more information on data loss prevention can be found in WCM Policy ITS-500.09 - *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 WCM alumni account.

7.02 Faculty

At the discretion of a department head, chairperson, or Human Resources, or Office of General Counsel, WCM faculty may be permitted to retain their email account for a temporary period after leaving WCM. 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 WCM 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.

7.03 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 WCM ends. Staff who transition from WCM to NewYork-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

References

- WCM Policy ITS-500.01 - Responsible Use of Information Technology Resources
- WCM Policy ITS-500.02 - Privacy of the Weill Cornell Medicine Network and Systems
- WCM Policy ITS-500.03 - Data Classification
- WCM Policy ITS-500.08 - Use of Email
- WCM Policy ITS-500.09 - Data Loss Prevention
- WCM Policy ITS-500.13 - Directory
- WCM Policy EA-120.01 - Personal Faculty Websites

Policy Approval

This policy was reviewed and approved by:

- Information Security and Privacy Advisory Committee (ISPAC) on June 4, 2026; and
- WCM-Executive Policy Review Group (WCM-EPRG) on June 16, 2026.

Version History

Date	Author	Revisions
12/15/2010		Initial draft completed
12/09/2014	Office of the CISO	Added transmission requirements for High Risk Data and delegation responsibilities
01/16/2015	Office of the CISO	Requires CIO approval for new email systems for business purposes
09/17/2015	Office of the CISO	Added provisions for email account retention
05/13/2023	Office of the CISO	Updated policy template and language; removed redundant sections
07/03/2024	Office of the CISO	Updated contact information and language
07/12/2024	Office of the CISO	Updated policy template and language
06/16/2026	Office of the CISO	Updated policy template and language, clarified clinician-patient communication methods and non-approved email systems, reinforced encryption requirements for High Risk Data, and added encryption guidance

Appendix

N/A