Weill Cornell Medicine	**Policy Title**	Privacy of the Weill Cornell Medicine Network and Systems
	Policy Number	500.02
	Department	ITS Security
	Effective Date	October 1, 2007
	Last Reviewed	July 23, 2024
	Last Updated	July 23, 2024
	Approved By	Tom Horton
	Approval Date	July 23, 2024

Policy

Weill Cornell Medicine provides, manages, and secures institutional equipment such as computers, tablets, or telephones, or organizational systems, such as email, communication software, internet access and usage, file sharing, document management or electronic medical record systems to community members to further the mission of education, research, and patient care and for conducting general college business. As part of your affiliation with Weill Cornell Medicine, you are responsible for using this equipment and systems consistent with this policy and Weill Cornell Medicine policy 500.01 – Responsible Use of Information Technology Resources.

While incidental and occasional personal use of such systems is permissible, personal communications and data transmitted or stored on Weill Cornell Medicine information technology resources are treated as business communications and data and are subject to monitoring for performance and compliance purposes. Automated monitoring systems may be used to flag communications, applications, user activity, and data that appear suspicious or malicious in nature (e.g., viruses, spyware) for further investigation. Weill Cornell Medicine community members should not expect that personal or business communications will remain private and/or confidential.

While the college allows unrestricted use of its information technology resources, users of Weill Cornell Medicine's IT resources should not expect privacy rights. The institution reserves the right to monitor all communications, data, and equipment used to access the organization's systems. Additionally, other institutions may monitor the use of our electronic medical record system and related data.

Purpose

Weill Cornell Medicine recognizes that an information technology environment built on mutual trust and freedom of thought is essential to the mission of education, research, and patient care. Weill Cornell Medicine additionally recognizes that as faculty, staff, and students create and store data in electronic form, there is concern that the data a user in the Weill Cornell Medicine community might consider private may be more available to view or use than initially expected. This policy is intended to clarify general principles and define expectations of privacy within the Weill Cornell Medicine community.

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.

Procedure

Weill Cornell Medicine reserves the right to access, review, quarantine, and release electronic information that is stored or transmitted using Weill Cornell Medicine information technology resources, including any devices you own or control which you use to access Weill Cornell Medicine systems or data or conduct Weill Cornell Medicine business. Requests for access, review, quarantine, or release of electronic information may originate from, or on behalf/approval of any of the following Weill Cornell Medicine officials:

- Associate Vice President, Deputy General Counsel and Secretary
- Chief Privacy & Clinical Compliance Officer
- Chief Information Security Officer
- Research Integrity Officer
- Senior Director, Human Resources Services
- Senior Associate Dean, Education
- Dean, Weill Cornell Graduate School of Medical Sciences

These requests will be initiated and fulfilled only under one or more of the following circumstances:

1. When requested by a court order or other entity with legal authority to do so.
2. When fulfilling the legal, regulatory, or other applicable duties of Weill Cornell Medicine.
3. When responding to a suspected or known electronic or physical security issue or incident.
4. In the event of a health or safety concern.
5. In order to ensure the security, confidentiality, integrity, or availability of data stored or transmitted by using Weill Cornell Medicine information technology resources.
6. In cases where more stringent controls, such as state regulations for psychiatric data, maintain a higher standard for authorized access, review, or release of data, the more stringent control will always take precedence.
7. As requested by the Office of General Counsel or University Audit Office in conducting investigations.

Whenever access, review, or release of electronic information is necessary, care will be taken to treat the event with sensitivity and respect.

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, 500.02– [Privacy of the Weill Cornell Medicine Network and Systems], to the Chief Information Security Officer, using one of the methods below:

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

Policy Approval

Version History

Date	Author	Revisions
October 1, 2007		Policy implemented
January 2, 2019	Brian J. Tschinkel	Updated tiles of WCM officials

March 18, 2022	Brian J. Tschinkel	Updated tiles of WCM officials
May 17, 2022	Brian J. Tschinkel	Updated policy statements
March 14, 2023	Tom Horton	Updated policy template
June 20, 2024	Tom Horton	Updated policy language and contact information
July 11, 2024	Christine Klucznik	Updated policy template