Weill Cornell Medicine

11.02

Privacy of the Weill Cornell Medicine Network and Systems

Responsible Executive: Chief Information Officer, Weill Cornell Medicine
Original Issued: October 1, 2007
Last Updated: March 14, 2023
Last Reviewed: March 14, 2023

Contents

Policy Statement

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 for the purpose of furthering 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 to use this equipment and systems consistent with this policy and Weill Cornell Medicine policy 11.01 – 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 permits generally unhindered use of its information technology resources, those who use Weill Cornell Medicine information technology resources do not acquire, and should not expect, a right of privacy. Consistent with these policies, the institution may monitor use of any and all communications and data and the equipment and communications made with any devices you own or control which you use to access the organization's data, software, network, or systems. Similarly, the use of our electronic medical record system, ancillary systems, and data may be monitored by other institutions with whom Weill Cornell Medicine shares that system.

Reason for Policy

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 growing 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 some general principles and define expectations of privacy within the Weill Cornell Medicine community.

Entities Affected by this Policy

All units of Weill Cornell Medicine, including Weill Cornell Medicine-Qatar.

Who Should Read this Policy

All members of the Weill Cornell Medicine community utilizing Weill Cornell Medicine information technology resources.
All stewards and custodians of Weill Cornell Medicine data.

Web Address of this Policy

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

Contacts

Direct any questions about this policy, 11.02 – Privacy of the Weill Cornell Medicine Network and Systems, to Brian J. Tschinkel, Chief Information Security Officer, using one of the methods below:

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

1. Principles

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 where possible.

Revision History:

Date	Author	Revision
October 1, 2007		Policy implemented
January 2, 2019	Brian J. Tschinkel	Updated titles of WCM officials
March 18, 2022	Brian J. Tschinkel	Updated titles of WCM officials
May 17, 2022	Brian J. Tschinkel	Updated policy statements
March 14, 2023	Brian J. Tschinkel	Updated policy template