11.02

Privacy of the Network

Responsible Executive: Chief Information Officer, WCM
Original Issued: October 1, 2007
Last Updated: January 2, 2019

Policy Statement
Weill Cornell Medicine (WCM) provides computer, email, network, internet, and telephone access to faculty, staff, and students 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 such systems is permissible, personal communications and data transmitted or stored on WCM information technology resources are treated as business communications, and are subject to automated surveillance by security systems managed by the Information Technologies and Services Department (ITS). Automated surveillance systems do not generally inspect content of data, but will flag data that appear malicious in nature (e.g. viruses, spyware) for further investigation. WCM community members should not expect that personal communications will remain private and/or confidential. 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.

Reason for Policy
WCM 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. WCM 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 WCM 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 WCM community.

Entities Affected by this Policy
The Weill Cornell Medical College and Graduate School of Medical Sciences

Who Should Read this Policy
All individuals provided with a CWID for accessing Weill Cornell Medicine information systems.

Web Address of this Policy
https://its.weill.cornell.edu/policies/

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

- Office: (646) 962-2768
- Email: brt2008@med.cornell.edu
Contents
1. Principles ............................................................................................................................................................................ 3
2. Definitions ........................................................................................................................................................................... 3
1. Principles
WCM reserves the right to access, review, and release electronic information that is stored or transmitted using WCM information technology resources. Requests for access, review, quarantine or release of electronic information may originate from, or on behalf/approval of any of the following WCM officials:

- Deputy University Counsel
- Chief Privacy Officer & Senior Billing Compliance Officer
- Chief Information Security Officer
- Research Integrity Officer
- Vice Dean of Weill Cornell Medical College
- Senior Director, Human Resources
- Senior Associate Dean of Education
- Dean of 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 WCM.
3. When responding to an 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, and availability of data stored or transmitted by WCM 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 precedent.
7. As requested by the University Audit Office in conducting investigations.

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

2. 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