Privacy of the Network

Policy Statement

Weill Cornell Medicine provides institutional equipment such as a computer, tablet, or telephone, or organizational systems, such as email, communication software, internet access and usage, file sharing, document management or electronic medical record systems to faculty, staff, and students 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 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. Weill Cornell Medicine 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 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 Weill Cornell Medicine data or the equipment and communications made with any devices you own or control which you use to access the organization's data, software, or systems, and the use of our electronic medical record system 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

Weill Cornell Medicine

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
### Revision History:

<table>
<thead>
<tr>
<th>Date</th>
<th>Author</th>
<th>Revision</th>
</tr>
</thead>
<tbody>
<tr>
<td>October 1, 2007</td>
<td></td>
<td>Policy implemented</td>
</tr>
<tr>
<td>January 2, 2019</td>
<td>Brian J. Tschinkel</td>
<td>Updated titles of WCM officials</td>
</tr>
<tr>
<td>March 18, 2022</td>
<td>Brian J. Tschinkel</td>
<td>Updated titles of WCM officials</td>
</tr>
<tr>
<td>May 17, 2022</td>
<td>Brian J. Tschinkel</td>
<td>Updated policy statements</td>
</tr>
</tbody>
</table>
Contents

1. Principles .................................................................................................................................................................... 5
1. Principles
Weill Cornell Medicine reserves the right to access, review, 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:

- Deputy General Counsel
- 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 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 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 precedent.
7. As requested by the Office of General Counsel or University Audit Office in conducting investigations.

Whenever access, review, or release of Weill Cornell Medicine data is necessary, care will be taken to treat the event with sensitivity and respect where possible.