

# Tracking Technologies

**Responsible Executive:** Chief Information Officer, Weill Cornell Medicine

**Original Issued:** May 31, 2023

**Last Updated:** September 25, 2023

**Last Reviewed:** September 25, 2023

---

## Contents

Policy Statement.....	2
Reason for Policy.....	2
Entities Affected by this Policy.....	2
Who Should Read this Policy.....	2
Web Address of this Policy.....	2
Contacts.....	2
1. Overview.....	3
2. Individual Responsibilities.....	3
2.01 Acceptable Use of Tracking Technologies.....	3
2.02 Reporting an Incident.....	3

## Policy Statement

In order to protect the security and integrity of Weill Cornell Medicine data, as well as to comply with applicable state and federal laws and regulations, Weill Cornell Medicine data must be adequately secured. Websites and applications that include the Weill Cornell Medicine brand (“applications”) shall not inappropriately collect and/or share any identifiable information with third-party entities. This policy applies to personally identifiable information, including the visitor’s IP address or their protected health information (“identifiable information”), collected by these applications.

## Reason for Policy

The purpose of this policy is to inform the Weill Cornell Medicine community as to what is permissible with respect to the creation or use of tracking technologies on websites and applications that include the Weill Cornell Medicine brand. Tracking technologies are used by institutions to collect and analyze information about how individuals interact with their websites or mobile applications. This information must be adequately secured and cannot be shared with third-party entities without appropriate protections and agreements in place.

## 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.  
All administrators of websites and applications that represent the Weill Cornell Medicine brand.

## Web Address of this Policy

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

## Contacts

Direct any questions about this policy, 11.21 – Tracking Technologies, to Brian J. Tschinkel, Chief Information Security Officer, using one of the methods below:

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



## 1. Overview

Many organizations use online tracking technologies supplied by third-party vendors such as Google and Facebook/Meta on applications to collect and analyze information about individuals' behavior, and to ensure applications are functioning properly. Such analysis can be used in beneficial ways to help improve the individual's experience while using the application. However, this tracking information may contain enough information about the individual to identify who they are to third-party vendors. Therefore, tracking technologies cannot be installed on applications without proper safeguards.

## 2. Individual Responsibilities

All administrators or owners of applications that represent an affiliation to Weill Cornell Medicine are responsible for complying with this policy. The type of applications covered by this policy include, but are not limited to:

- Websites, whether publicly accessible (“unauthenticated”) or protected (“authenticated”), including the official public facing websites of Weill Cornell Medicine, as well as department, division, and lab websites, and personal healthcare-related portfolio websites that represent an affiliation to Weill Cornell Medicine
- Web and mobile applications, whether developed internally by Weill Cornell Medicine or a third-party, that represent an affiliation or are used in a manner associated with Weill Cornell Medicine

The Information Technologies & Services Department (ITS) will maintain compliance with this policy for applications under their management. Owners and administrators of websites and web or mobile applications not managed by ITS that represent they are affiliated with Weill Cornell Medicine, either in text or by use of Weill Cornell Medicine branding, must ensure compliance with this policy. ITS is available to assist in complying with this policy upon request.

### 2.01 Acceptable Use of Tracking Technologies

Tracking technologies may be used on applications after completion of Security and Privacy reviews. The reviews will ensure that all collections or disclosures of identifiable information follow federal, state, and local laws and regulations and only the minimum information necessary is disclosed to achieve the intended purpose. Subsequent changes to the configuration of tracking technologies after approval will require new compliance reviews.

At a minimum, Weill Cornell Medicine requires that the use of tracking technologies be disclosed in the application's privacy policy or terms and conditions of use. Furthermore, if any identifiable information will be exchanged with a third party, individuals must work with the Compliance & Privacy Office to evaluate whether a business associate or other privacy agreement is necessary prior to any disclosure of identifiable information. The execution of a privacy agreement will also require a security risk assessment of the third party.

Weill Cornell Medicine reserves the right to remove tracking technologies from its applications that do not have the appropriate safeguards in place.

### 2.02 Reporting an Incident

Individuals who suspect or know of violations of this policy should immediately report the incident to ITS Support. Even if the violation is not confirmed, it is imperative that the incident is reported quickly so the right personnel can investigate as soon as possible.



To report an incident, notify ITS Support:

ITS Support  
T (212) 746-4878  
[support@med.cornell.edu](mailto:support@med.cornell.edu)

If you wish to notify a compliance office directly or to report the incident anonymously, the following contacts can be used:

Compliance & Privacy Office  
T (646) 962-6930  
[privacy@med.cornell.edu](mailto:privacy@med.cornell.edu)

ITS Security  
T (646) 962-3010  
[its-security@med.cornell.edu](mailto:its-security@med.cornell.edu)

Cornell Hotline (Anonymous)  
T (866) 293-3077  
<http://hotline.cornell.edu>

Filing or reporting an incident can be done without fear or concern of retaliation.



**Revision History:**

<b>Date</b>	<b>Author(s)</b>	<b>Revision</b>
September 25, 2023	C. Dor, N. Grodd, C. O'Connor, M. Joseph, L. Bradford, B. Tschinkel, J. Barber, S. Singer	Initial draft completed

