11.06

Device Encryption

Responsible Executive: Chief Information Officer, Weill Cornell Medicine
Original Issued: July 15, 2008
Last Updated: September 15, 2023
Last Reviewed: September 15, 2023

Contents

Policy Statement

All members of the Weill Cornell Medicine community must take care to protect high risk data on their laptops, desktops, smartphones, and tablets (“devices”). All devices owned by Weill Cornell Medicine must be encrypted, and devices not owned by Weill Cornell Medicine but used for Weill Cornell Medicine purposes must adhere to the appropriate safeguards defined in this policy to protect high risk data. All removable storage drives, such as external hard drives or USB flash drives, must be encrypted if containing high risk data. Any variances to this policy must meet the requirements defined in ITS policy 11.20 – Variances.

Reason for Policy

Encryption provides strong protection by making data inaccessible to those without proper access credentials. Additionally, encryption can exempt Weill Cornell Medicine from reporting requirements in the event of a theft or loss under the Information Security Breach and Notification Act, and it meets many of the security standards defined under the HIPAA Security Rule.

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, 11.06 – Device Encryption, to Brian J. Tschinkel, Chief Information Security Officer, using one of the methods below:

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

1. Encryption of Devices Owned by Weill Cornell Medicine

Encryption shall be provided, at no additional charge, for all institutionally owned devices used by the Weill Cornell Medicine community that are not otherwise exempted from this rule.

2. Encryption of Devices Not Owned by Weill Cornell Medicine

Pursuant to ITS policy 11.10 – Device Minimum Security Requirements, individuals are responsible for safeguarding Weill Cornell Medicine data on devices not owned or issued by Weill Cornell Medicine. Such devices may include personally owned devices, individual devices owned by another institution, or publicly available devices such as those in a library, café, or hotel business center.

Individuals must ensure whole-disk encryption is enabled on their personally owned devices or individual devices owned by another institution if they will be using the devices to access or store high risk data. These devices must also be registered with ITS in the High Risk Attestation.

Devices available for public use, such as those in a library, café, or hotel business center, will often not support encryption and must only be used temporarily for Weill Cornell Medicine purposes. Individuals are responsible for taking appropriate precautions to ensure Weill Cornell Medicine data is not saved locally or accessible by others.

A security or privacy breach that results in the compromise of data from a device not owned by Weill Cornell Medicine may have severe consequences.

ITS is available to assist and provide “best effort” support to encrypt devices not owned by Weill Cornell Medicine. Devices owned by another institution, such as those which are owned by affiliates of Weill Cornell Medicine, should utilize the encryption software approved by that institution’s IT department. Individuals are strongly encouraged to make a backup of the personal data on their device and verify it for accuracy and completeness before seeking assistance from ITS to encrypt their device for Weill Cornell Medicine purposes.

3. Removable Storage Devices

High risk data stored on removable storage devices must be encrypted. Examples of removable storage devices include, but are not limited to, flash drives, external hard drives, memory cards, and optical discs. Strong hardware- or software-based encryption algorithms such as the Advanced Encryption Standard (AES) with at least 256-bit keys should be used. Examples of compliant encryption software for removable storage devices include Apple FileVault 2, Microsoft BitLocker, LUKS (for Linux systems), and VeraCrypt (open source). When encrypted removable storage devices are used to share high risk data, the encryption password must be shared separately and in a secure manner, such as encrypted email.

4. Variances to this Policy

There is significant risk in not encrypting devices used to access Weill Cornell Medicine data and a breach may result in regulatory sanctions and fines for the college and the individual responsible for the data. Variances shall be considered in relatively unusual circumstances and must meet the requirements defined in ITS policy 11.20 – Variances.

5. Device Decommission and Decryption

Upon leaving Weill Cornell Medicine, individuals with devices owned by Weill Cornell Medicine must turn their devices into their supervisor. These devices will remain encrypted and will be securely repurposed or reprovisioned. Individuals with devices not owned by Weill Cornell Medicine which have been used for Weill Cornell Medicine purposes must inform ITS and their supervisor prior to termination so that Weill Cornell Medicine data can be removed; the devices can then be decrypted.

Revision History:

Date	Author	Revision
July 15, 2008		Initial draft completed
October 3, 2014	Brian J. Tschinkel	Expanded policy to expand to end user devices beyond laptops; clarified exemptions
January 4, 2015	Brian J. Tschinkel	Modified guidelines for exemptions
November 8, 2018	Brian J. Tschinkel	Removed references to obsolete ITS services
September 7, 2021	Brian J. Tschinkel	Added *Revision History* and *Removable Storage Devices* sections
May 11, 2023	Brian J. Tschinkel	Updated policy template and language for branding
May 13, 2023	Brian J. Tschinkel	Changed nomenclature around “tagged” and “untagged” to ownership
September 12, 2023	Brian J. Tschinkel	Added reference to new policy for variances
September 15, 2023	Brian J. Tschinkel	Ensured consistent language with 11.10 policy