Device Encryption

Responsible Executive: Chief Information Officer, Weill Cornell Medicine

Original Issued: July 15, 2008
Last Updated: May 13, 2023
Last Reviewed: May 13, 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. Encryption of Devices Owned by Weill Cornell Medicine........................................................................... 3
2. Encryption of Devices Not Owned by Weill Cornell Medicine ...................................................................... 3
3. Removable Storage Devices ............................................................................................................................ 3
4. Variances to this Policy ................................................................................................................................... 3
5. Device Decommission and Decryption........................................................................................................ 4
**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 within and must be recertified on an annual basis.

**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

Users are responsible for safeguarding high risk data on devices not owned by Weill Cornell Medicine that are used for Weill Cornell Medicine purposes. Such devices may include individually- or personally-owned devices, devices owned by another institution, or publicly available devices such as those in a library, café, or hotel business center. In situations where an individual needs to access Weill Cornell Medicine high risk data from a device not owned by Weill Cornell Medicine, secure channels shall be used. Examples of known secure channels are ITS-supported remote access connections (such as myApps), Wi-Fi networks secured with a password (not in public cafés or hotels), or Office 365 Outlook on the web ("webmail"). Users shall take caution to not download or save sensitive attachments or files on these devices. 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. In extenuating circumstances where high risk data must be stored on these devices, the devices should be encrypted to ensure the confidentiality of the data. Users are responsible for identifying these devices in the annual High Risk Attestation.

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. Users 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

Variances shall be considered in relatively unusual circumstances only when any of the following conditions are met and compensating controls can be applied:

1. The device is demonstrated not to contain high risk data;
2. Users attest that the device will never be used for high risk data;
3. The device does not meet the minimum hardware requirements to support encryption or is known to be incompatible with a Weill Cornell Medicine application;
4. No practical encrypted alternative is available; and,
5. A completed variance request form is submitted to ITS with approval from the user’s department administrator.

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.

Any devices with an approved variance to this policy that change possession or are repurposed must be encrypted or filed under a new variance request. Variances must be renewed and recertified on an annual basis.
5. Device Decommission and Decryption

Upon leaving Weill Cornell Medicine, users 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. Users 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:

<table>
<thead>
<tr>
<th>Date</th>
<th>Author</th>
<th>Revision</th>
</tr>
</thead>
<tbody>
<tr>
<td>July 15, 2008</td>
<td>Initial draft completed</td>
<td></td>
</tr>
<tr>
<td>October 3, 2014</td>
<td>Brian J. Tschinkel</td>
<td>Expanded policy to expand to end user devices beyond laptops; clarified exemptions</td>
</tr>
<tr>
<td>January 4, 2015</td>
<td>Brian J. Tschinkel</td>
<td>Modified guidelines for exemptions</td>
</tr>
<tr>
<td>November 8, 2018</td>
<td>Brian J. Tschinkel</td>
<td>Removed references to obsolete ITS services</td>
</tr>
<tr>
<td>September 7, 2021</td>
<td>Brian J. Tschinkel</td>
<td>Added Revision History and Removable Storage Devices sections</td>
</tr>
<tr>
<td>May 11, 2023</td>
<td>Brian J. Tschinkel</td>
<td>Updated policy template and language for branding</td>
</tr>
<tr>
<td>May 13, 2023</td>
<td>Brian J. Tschinkel</td>
<td>Changed nomenclature around “tagged” and “untagged” to ownership</td>
</tr>
</tbody>
</table>