Weill Cornell Medicine

11.06

Device Encryption

Responsible Executive: Chief Information Officer, WCM
Original Issued: July 15, 2008
Last Updated: September 7, 2021

Policy Statement

All users of desktops, laptops, tablets, and mobile devices (whether Information Technologies & Services [ITS] tagged or untagged) must take care to protect high risk data. All devices tagged by ITS and used for WCM purposes must be encrypted using an ITS-approved encryption solution unless a variance has been submitted and approved as defined in this policy. Users shall take care when accessing, storing, or transmitting high risk data on untagged devices, as described in this policy. All untagged removable storage drives, such as external hard drives or USB flash drives, must be encrypted if containing high risk data.

Reason for Policy

Encryption provides strong protection by making data inaccessible to those without proper access credentials. Additionally, encryption can exempt WCM 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

Weill Cornell Medicine

Who Should Read this Policy

All individuals accessing, storing, sending, receiving, or transmitting any WCM 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

Contents

Revision History

Date	Comment
July 15, 2008	Initial version
⋮	
September 7, 2021	Added *Revision History* and *Removable Storage Devices* sections

1. Encryption of Supported Devices

Encryption shall be provided, at no additional charge, for any tagged device used by WCM faculty, staff, students, administrative officials or, in select cases, affiliates that is not otherwise exempted from this rule.

WCM faculty, staff, students, and affiliates with encrypted devices who are terminating their relationship with the medical college must inform ITS or their department head prior to termination so that the encryption software and confidential data can be safely removed.

2. Encryption of Unsupported Devices

Users are responsible for safeguarding high risk data on untagged devices, such as those that are individually or personally owned but used for WCM purposes. In situations where an individual needs to access WCM high risk data from an untagged device, secure channels shall be used. Examples of known secure channels are ITS-supported remote access connections, Wi-Fi networks secured with a password (not in public cafés or hotels), or webmail. Users shall take caution to not download or save sensitive attachments or files on untagged devices. In extenuating circumstances where high risk data must be stored on untagged devices, the devices should be encrypted to ensure the confidentiality of the data. Users of untagged and unencrypted devices are responsible for safeguarding and securing WCM high risk data.

ITS is available to assist and provide “best effort” support to encrypt untagged devices. Users are strongly encouraged to make an encrypted backup of the device data and verify it for accuracy and completeness.

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

All end user devices (regardless of individual or college ownership) must be encrypted if they access, store, send, or receive high risk data. Variances shall be considered in relatively unusual circumstances only when the following conditions are met:

1. The device is demonstrated not to contain protected data at least annually and users attest that it will never be used for protected data;
2. The device does not meet the minimum hardware requirements to support encryption or is known to be incompatible with a WCM application;
3. No practical encrypted alternative is available; and,
4. A completed variance request form is submitted to ITS Support with approval from the user’s department administrator.

There is significant risk in not encrypting devices used to access WCM 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.

5. Device Decommission and Decryption

Users leaving WCM must notify ITS in advance of leaving so any managed encryption software and high risk data can be safely removed. Contact ITS Support to schedule the removal.

6. Additional Resources

- Asset Disposal Form
- Variance Request Form

7. Related Policies

- 11.03 – Data Classification
- 11.17 – Identity and Access Management

8. 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
- PII — Personally identifiable information, as defined in GAO-08-536 Privacy Protection Alternatives, is any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.
- PHI — Protected health information, as defined in Title 45 CFR §160.103, is individually identifiable health information that is (i) transmitted by electronic media; (ii) maintained in electronic media; or (iii) transmitted or maintained in any other form or medium. Protected health information excludes individually identifiable health information (i) in education records covered by the Family Educational Rights and Privacy Act (FERPA), as amended, 20 U.S.C. 1232g; (ii) in records described at 20 U.S.C. 1232g(a)(4)(B)(iv); (iii) in employment records held by a covered entity in its role as employer; and (iv) regarding a person who has been deceased for more than 50 years.
- HIPAA — Health Insurance Portability and Accountability Act of 1996.
- high risk data — As defined in ITS 11.03 – Data Classification, high risk data includes, without limitation, the following: PHI; PII; financial data, including data covered under the Gramm-Leach-Bliley Act (GLBA) and the information pertaining to credit cards

	covered by the Payment Card Industry Data Security Standard (PCI DSS); employment records, including pay, benefits, personnel evaluations, and other staff records; research data involving human subjects that are subject to the Federal Policy for the Protection of Human Subjects (Common Rule) as defined in Title 45 CFR §46.101 et seq.; and user account or system passwords that provide access to information systems or applications containing any of the above confidential data elements.
• tagged device	A tagged device that is supported by ITS and is permitted to connect to the WCM network and access selected WCM services.
• untagged device	A device that is not supported by ITS and is not permitted to connect to the WCM network.
• removable storage	A portable storage device such as a floppy disk, compact disk, USB flash drive, external hard drive, and other flash memory card/drive that contains nonvolatile memory.
• encryption	A process which converts plain data into a coded form or cipher in order to prevent unauthorized access.