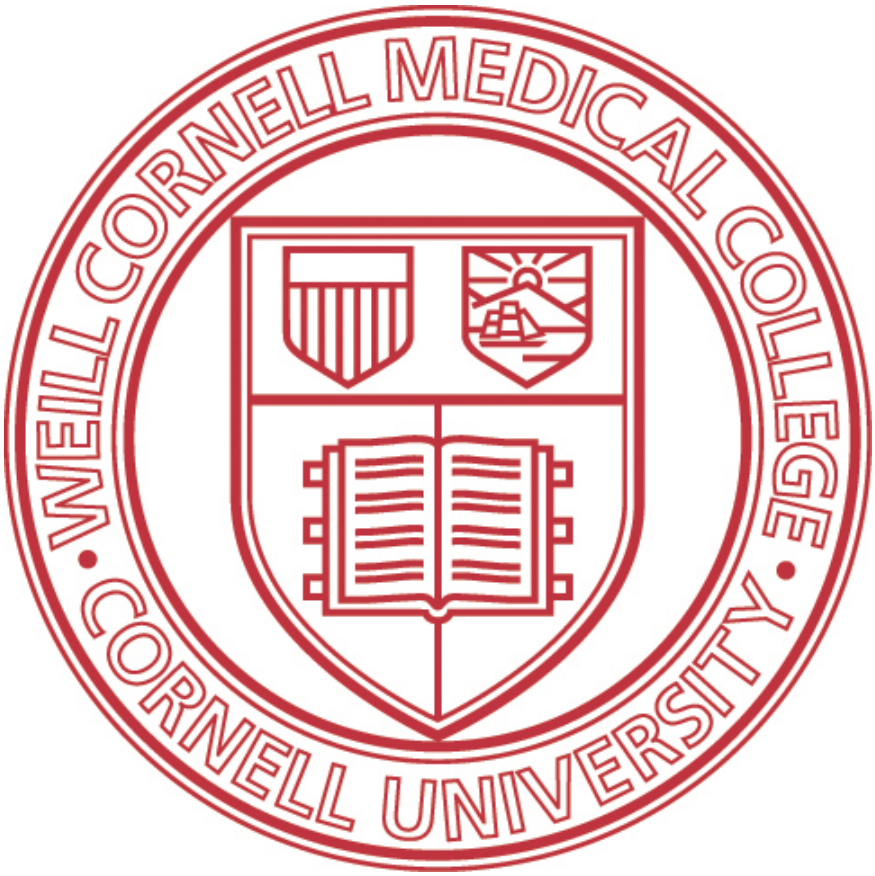

ITS Policy Library

11.06 - Device Encryption

Information Technologies & Services

Responsible Executive:	Chief Information Officer, WCMC
Original Issued:	July 15, 2008
Last Updated:	November 21, 2014

Policy Statement

All users of desktops, laptops, tablets, and mobile devices (whether Information Technologies & Services [ITS] tagged or untagged) must take care to protect confidential data. All devices tagged by ITS and used for WCMC purposes must be encrypted using an ITS-managed encryption solution unless otherwise exempted as defined in this policy. Users shall take care when accessing, storing, or transmitting confidential 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 confidential data.

Reason for Policy

Encryption provides strong protection by making data inaccessible to those without proper access credentials. Additionally, encryption can exempt WCMC 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 Medical College and Graduate School of Medical Sciences

Who Should Read this Policy

All individuals accessing, storing, sending, receiving, or transmitting any WCMC data.

Web Address of this Policy

http://weill.cornell.edu/its/policy/security/116---laptop-encryption.html

Contacts

Direct any questions about this policy, 11.06 - Device Encryption, to Brian J. Tschinkel, Information Security Officer, using one of the methods below:

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

Definitions

These definitions apply to terms as they are used in this policy.

i) ITS	Information Technologies & Services Department
ii) WCMC	Weill Cornell Medical College
iii) 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.
iv) 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.
v) HIPAA	Health Insurance Portability and Accountability Act of 1996.
vi) confidential	As defined in ITS 11.03 – Data Classification, confidential data includes, without limitation, the following: PHI; PII; student records, including those protected under the Family Education Rights and Privacy Act (FERPA), as amended, 20 U.S.C. 1232g; 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 research grants and related information, such as applications, contracts, study protocols (including those involving animals), intellectual property belonging

	to Weill Cornell Medical College, and other sensitive research data.
vii) tagged device	A device that is supported by ITS and is permitted to connect to the WCMC network and access selected WCMC services.
viii) encryption	A process which converts plain data into a coded form or cipher in order to prevent unauthorized access.

I. Principles

Section 1.01 **ENCRYPTION OF SUPPORTED (TAGGED) DEVICES**

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

WCMC 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.

Section 1.02 **ENCRYPTION OF UNSUPPORTED (UNTAGGED) DEVICES**

Users are responsible for safeguarding confidential data on untagged devices, such as those that are individually or personally owned but used for WCMC purposes. In situations where an individual needs to access WCMC confidential data from an untagged device, secure channels shall be used. Examples of known secure channels are ITS-supported VPN and webVPN connections, Wi-Fi networks secured with a password (not in public cafés or hotels), the ITS virtual desktop and Citrix thin client access service, myDesktop (http://weill.cornell.edu/mydesktop), or webmail. Users shall take caution to not download or save sensitive attachments or files on untagged devices. In extenuating circumstances where confidential 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 WCMC confidential 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.

Section 1.03 **EXEMPTION GUIDELINES FOR DEVICES THAT DO NOT MEET ENCRYPTION STANDARDS**

All desktops, laptops, tablets, and mobile devices, whether individually owned or distributed by ITS and accessing, storing, sending, or receiving confidential data, must be encrypted. Exemptions 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 WCMC application;
3. No practical encrypted alternative is available; and,

4. A completed Request for Device Encryption Exemption form is submitted to ITS Support with approval from the user's Department Administrator or Chair.

There is significant risk in not encrypting devices used to access WCMC data and a breach may result in regulatory sanctions and fines for the college and the individual responsible for the data.

Any exempted devices that change possession or are repurposed must be encrypted or filed under a new exemption request.

II. Procedures

Section 2.01 **REQUESTING ENCRYPTION FOR UNTAGGED DEVICES**

To have encryption enabled on an untagged desktop, laptop, tablet, or mobile device, users should:

1. Backup all valuable data on their device, including email and documents. ITS can assist with this for supported devices but only a user can confirm that the backup is valid and adequate. Backups containing confidential data should be encrypted or stored on a secure server or in a locked cabinet.
2. Fill out and submit the device encryption form. A member of the ITS Service Desk will contact you to arrange the installation.
3. If not already done, sign into myPassword and complete the account setup process.

All devices tagged subsequent to the issuance of this policy will be encrypted by default unless one or more of the exception criteria are met.

Section 2.02 **LEAVING WCMC/REMOVING ENCRYPTION**

Users leaving WCMC must notify ITS in advance of leaving so any managed encryption software and confidential data can be safely removed. Contact support@med.cornell.edu to schedule the removal.

If the encryption software causes unforeseen problems, contact support@med.cornell.edu for assistance.

III. Related Documents

The following documents are also relevant to this policy:

ix) 11.03 – Data Classification