Weill Cornell Medicine
Information Technologies & Services

Request for Device Encryption Exemption Form

ITS Incident Number:	
Request Date:	
Requestor's Name:	
Requestor's CWID:	
Requestor's Title:	
Requestor's Division:	
Requestor's Department:	
Department Administrator:	
Requestor's Device Tag:	
Are there applications on the system that are incompatible with encryption? **If there are any incompatibilities, documentation from the vendor must be provided.**	
What type of device (e.g., laptop, desktop, smartphone, tablet) is being requested for exemption **and** what is the operating system (e.g., Windows 7, Mac OS X, iOS 8, Android 4.4)?	
Does the device contain any protected health information[1] (PHI)? If so, please describe the data and its purpose.	
Does the device contain any personally identifiable information[2] (PII)? If so, please describe the data and its purpose.	

[1] 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.

[2] 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.

Does the device contain any confidential[3] data other than PHI or PII as described in the 11.03 – Data Classification policy? If so, please describe the data and its purpose.	
Does the device contain any grant applications, study protocols, animal study information, intellectual property, or other sensitive research data or information? If so, please describe the data and its purpose.	
Is the device "portable" whereby it can or may be transferred from its location to another WCM area or outside of the WCM facilities?	
Will the device be reviewed, supported, and/or inspected by a third party?	
Is the device connected to the WCM network or does it access any other system, application, or share that resides on the WCM network?	
How is the device physically secured (e.g., in a locked office, secured from tampering, bolted to a desk, etc.)? **Physical safeguards are required as a countermeasure against theft for hard drives that cannot be encrypted.**	

Terms and Conditions

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 WCM application;*
3. *No practical encrypted alternative is available; and,*
4. *A completed Request for Device Encryption Exemption form is submitted ITS Support with approval from the user's Department Administrator, Chair, or Director.*

[3] As defined in ITS 11.03 – Data Classification, confidential data includes data protected by state and/or federal law against unauthorized use, disclosure, modification, destruction. Confidential data includes, without limitation, the following: (a) patient billing or medical records (in any electronic form, including but not limited to: databases, spreadsheets, audio/video recordings, transcripts, etc.), including data covered by the Security Rule of the Health Insurance Portability and Accountability Act (HIPAA); (b) student records, including those protected under the Family Education Rights and Privacy Act (FERPA); (c) 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); (d) employment records, including pay, benefits, personnel evaluations, and other staff records; (e) research data involving human subjects that are subject to the Common Rule (Federal Policy for the Protection of Human Subjects, 46 CFR 101 et seq); and (f) Social Security Numbers.

Weill Cornell Medicine
Information Technologies & Services

Request for Device Encryption Exemption Form

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.

In situations where an exemption is granted based upon no access to confidential data, the requestor must attest that personally identified information, protected health information, or WCM confidential data as described in the WCM Data Classification Policy is not accessed or stored from this device. If the requestor's job responsibilities or the use of the device changes where access to PII, PHI, or confidential data is necessary, the device will then need to be encrypted and the exemption will no longer be valid. This attestation must be completed annually. In addition to approval by ITS Security, the Department Administrator/Chair/Director must approve this request.

Any exemption denials may be appealed by the requestor and will be brought to and reviewed by the Information Security and Privacy Advisory Committee (ISPAC). All requests must be reviewed and recertified on an annual basis.

Requestor's Name (Printed): _____

Requestor's Signature: _____

Date of Signature: _____

Department Administrator/Chair/Director's Name (Printed): _____

Department Administrator/Chair/Director's Signature: _____

Date of Signature: _____

FOR ITS USE ONLY:

Request Approved (Yes or No): _____

Request Approved By (Printed Name): _____

Request Approved By (Signature): _____

Approved Date: _____