1. Purpose and Scope

The purpose of this policy is to comply with federal and state regulations governing privacy and security of information processed, transmitted or stored on all laptop computers that will be used for UMMC purposes. This policy is to provide compliance with security best practices and to protect confidential and/or sensitive data in the event of lost or stolen laptop computer.

All UMMC owned laptops and all other similar devices providing some or all of the laptop capabilities are governed by this policy.

Encryption supports data privacy and integrity by providing a method to convert electronic information into a format that is readable only by authorized individuals. This policy establishes that use of full disk encryption for electronic information in storage shall be consistent with the campus need for continued availability of the information. This policy applies to all clinical, academic, research areas and their users. It applies to all UMMC owned laptop computers whether purchased as part of a grant or not. In addition this policy applies to all laptops used by the School of Pharmacy Department of Pharmacy Practice, including all laptop computers used by any of the various departments or schools that process, capture or contain patient data.

2. Definitions

A. Cryptography – a method used to encode information so that only authorized individuals can read the information
B. Full disk encryption (FDE) – the application of encryption to an electronic storage system and may exclude a system and/or boot partition
C. Electronic storage media – Electronic storage system used to record, index,
store, preserve, or retrieve data files, including portable storage systems.
D. Encryption – Transforming information using a secret key so that the
information is unintelligible to unauthorized parties.
E. See UMMC Data Classification Policy for definitions of types of data
(confidential, sensitive, and public).

3. Policy

All users of laptop computers or other electronic data mobile devices must use
reasonable care, as outlined in the UMMC’s Information Policy, to protect UMMC
confidential or sensitive data (as defined in the UMMC Data Classification
Protection of confidential data against physical theft or loss, electronic invasion,
or unintentional exposure is provided through a variety of means. These include
user care and a combination of technical protections such as encryption. These
work together to secure a computer against unauthorized data access. Prior to
the use of confidential data via laptop computer or other electronic data mobile
device, users are responsible for contacting the Division of Information Systems
to obtain appropriate protections for such computers or devices, or for verifying
that such protections are already in place. The use of any unsecured laptop to
access confidential and/or sensitive data is strictly prohibited, regardless
of whether the equipment is owned by UMMC or not.

   a. Laptops left unattended must be tethered or attached to the user’s desk or
      work surface to prevent theft.
   b. All UMMC owned laptops must be fully encrypted with the DIS approved
      encryption software prior to use unless exempted.
   c. All UMMC laptops must have DIS approved tracking software installed and
      enabled (ComputrACE).
d. All new or refurbished laptop computers received at UMMC must be delivered to an installation point (laptop depot) designated by DIS.

e. These laptop computers must have encryption (unless exempted) and device tracking (Computrace) enabled at the laptop depot location prior to delivery to the end user. Once properly configured and encrypted the laptop may then be distributed to the end user.

f. Electronic Protected Health Information (EPHI) must not be stored on any non-encrypted laptop computer.

g. All nonexempt laptop computers not capable of utilizing FDE must be disabled and removed from service.

h. The storage disk of any laptop computer removed from service must have the hard drives rendered un-useable prior to disposal.

4. Exemption

The Institutional Compliance Committee has mandated that all laptop computers being used for UMMC business and that are no older than 5 years old be encrypted. Every UMMC owned laptop computer and/or laptop computer used for UMMC purposes (including those belonging to Ole Miss or other institutions and/or personal laptops used for UMMC business) will either need to be encrypted or have an attestation statement saying the laptop computer has been exempted. An annual audit will be performed to ensure that all UMMC owned laptop computers are either encrypted or have an up-to-date attestation statement affirming the laptop computer does not contain confidential or sensitive data. Only laptops which have never and will never contain confidential and/or sensitive data may be considered for exemption.

Exemptions may be requested by completing the ‘Encryption Exemption Request Form for Laptop Computers’ (See Supplemental Document A). Once completed, the form must be submitted to the department chair/department head. The forms
will then be forwarded to the Compliance Committee or Compliance Committee designee for review to determine which laptops merit an exemption. (See Supplemental Document B) Once exempted, the laptop must be labeled with a sticker denying its use for storage of any confidential data and/or sensitive data.

If there is any doubt about a particular laptop computer being exempted, the department shall submit a request for exemption.

Any laptop computer that is exempted will be marked as “Not suitable for confidential or sensitive data as defined by the Laptop policy.” Any exempt laptop computer that changes possession/user must be encrypted or have an updated signed attestation statement. Any laptop computer that is repurposed to contain confidential or sensitive data must be encrypted.

5. Lost or Stolen Laptops

In the event a laptop computer that contains UMMC confidential or sensitive data is lost or stolen, the theft or loss must be reported immediately to the Campus Police Department, the UMMC Office of Integrity and Compliance and the Office of Information Security (OIS).

6. Sanctions

Individuals violating the UMMC Information Policy are subject to disciplinary action, up to and including termination. All violations must be reported to the Department of Internal Audit and OIS. Employee violations must be reported to the Department of Human Resources; student violations must be reported to the dean of the appropriate school. The intentional reporting of false violations will be treated as a violation. UMMC strictly prohibits retaliatory action against
individuals reporting violations.

7. Contact Information

For questions about the UMC Information Policy or for more information, send an email to OIS (UMC–Information-Security@dis.umc.edu), call the Office of Information Security at 984-1140, or call the Office of Integrity and Compliance at 815-3944.

8. Supplemental Documents

Supplemental Document A
Encryption Exemption Request Form for Laptop Computers

Supplemental Document B
Guidelines for Determining Exemption from Encryption