I. PURPOSE
To establish a policy governing the use of portable electronic equipment in order to safeguard confidentiality, protect LUMC’s proprietary information and to meet applicable state and federal laws and regulatory standards.

II. DEFINITIONS/APPLICATIONS
A. Definitions:
"Electronic Media" includes, but is not limited to: diskettes, CDs, data DVD’s, memory sticks, memory cards, laptops, personal digital assistants, pocket organizers, music players that act as mass storage devices, removable disk drives, magnetic tape, etc.

"Protected Health Information" or "PHI" is any health information that can be used to identify a patient and relates to health-care services provided to the patient, or the payment for those services. PHI includes: 1) All medical records and other information which identifies that patient, including demographic, medical and financial information; and 2) information in any form whether electronic, paper or spoken.

"LUMC Proprietary Information" includes, but is not limited to, Loyola records or documents and confidential information related to employees, students, faculty, volunteers, patients, research subjects, outside vendors, and contracting entities.

"Personal Information" is personal information as defined by the Illinois Personal Information Protection Act. The act defines "Personal information" as an individual’s first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:
1. Social Security Number.
2. Driver’s license number or State identification card number.
3. Account number or credit or debit card number, or an account number
   or credit card number in combination with any required security code,
   access code, or password that would permit access to an individual’s
   financial account.

"Personal information" does not include publicly available information that
is lawfully made available to the general public from federal, State, or local
government records.

“Transmitting electronic information” includes, but is not limited to,
electronic mail, file transfers, and web page transfers.

Workforce—For purposes of this policy and pursuant to 45 CFR 160.103,
Workforce includes employees of Loyola University Health System
(“LUHS”), Loyola University Medical Center (“LUMC”), Loyola University
Physician Foundation (“LUPF”) and Loyola University of Chicago (“LUC”)
working on the Maywood Campus and at the ambulatory care sites and
also includes the following: students, members of the Medical Staff,
volunteers, and agency or temporary staff receiving or performing services
on behalf of the Loyola entities.

B. Applications:
   This policy applies to the Workforce as defined in this policy.

III. PROCEDURES/INFORMATION
Prior to downloading, storing, maintaining, transmitting or transferring data
that includes PHI, LUMC Proprietary Information or Personal Information from
an LUMC network or personal computer to a form of Electronic Media, the
member of the Workforce must be sure that storage of PHI on a portable
device is absolutely required. Alternatives such as accessing a system
remotely using secure remote access (VPN) should be considered.

If the PHI, LUMC Proprietary Information, or Personal Information that is
obtained from an LUMC source and/or downloaded from an LUMC network or
personal computer should be placed on some form of Electronic Media, which
is used at or taken from a LUMC facility or transmitted out of LUMC, the
media must be protected using the means, as appropriate, listed below:

Encryption and password protection. The best protection is encryption using
the Advanced Encryption Standard (AES) with an encryption key or password
that is at least 128-bits in length. If data are transmitted, the password must
be sent using a non-electronic medium: letter, phone call, personal
conversation, or through a separately encrypted electronic message.
Password protection. Files like Excel worksheets and Access databases can be protected by passwords. The password must not be physically associated with the medium. Passwords must be at least eight characters in length and must not be obvious. Personal digital assistants and pocket organizers provide for passwords, which MUST be used to protect data.

Physical security. Workforce must keep track of such Electronic Media to ensure the Electronic Media is not misplaced and/or that unauthorized individuals do not have access to the Electronic Media.

Before replacing or disposing of Electronic Media containing PHI, LUMC Proprietary Information or Personal Information, the Workforce must use disk-wiping software to clear out or overwrite the PHI. This process must be in conformance with existing LUMC policy.

Information Technologies has several tools to encrypt information. Please contact the Help Desk to request information about such tools.

IV. VIOLATIONS
Administrators, Information System Staff, faculty, support staff, students, residents and others, as applicable, shall comply with this policy and its related procedures.

A. Intentional Violations. Any of these individuals who intentionally violate this Policy will be subject to the following, as applicable:
   1. Medical Staff will be subject to disciplinary action as determined by the LUPF Peer Review, Professional Standards and Compliance Committee.
   2. LUC faculty working on the medical center facilities that are not members of the Medical Staff will be subject to disciplinary action as described in the LUC faculty handbook.
   3. Medical Residents will be subject to disciplinary action as determined by the LUMC Chief of Staff Office.
   4. LUC students will be subject to disciplinary action as described in the LUC student handbook.
   5. Other students may be subject to possible dismissal from the LUMC or LUC educational programs.
   6. All remaining employees will be subject to the progressive disciplinary process, the Rules of Conduct outlined in the Employee Handbook and Loyola’s Corrective Action and Work Improvement Policy.

B. Unintentional Violations. Training related to unintentional breaches will be considered on a case-by-case basis. Violations may also be subject to civil, monetary and criminal penalties.
LOYOLA UNIVERSITY MEDICAL CENTER
ADMINISTRATIVE POLICY NUMBER: IT-006

V. RESPONSIBILITY
Any questions or concerns regarding this policy must be directed to the Chief Information Security Officer at extension 6-3333.