WESTERN MICHIGAN UNIVERSITY

ADMINISTRATIVE, TECHNICAL AND PHYSICAL SAFEGUARDS FOR THE
USE AND SECURITY OF PORTABLE ELECTRONIC STORAGE DEVICES
AND LAPTOP COMPUTERS

ALL UNIVERSITY COVERED ENTITIES

POLICY: The HIPAA Privacy Rules require that the University have appropriate
administrative, technical and physical safeguards to protect the privacy of
protected health information (PHI). More specifically the Rules require
that the University have in place reasonable safeguards to protect PHI
from intentional or unintentional use or disclosure that is in violation of
the Privacy Rules. Accordingly, the University adopts the following
procedures regarding the use and security of portable electronic storage
devices, such as, but not limited to, flash drives, memory sticks, data
disks, and laptop computers.

PROCESS:

1. All members of the workforce shall follow the measures set forth below
when they maintain PHI on portable electronic storage devices and/or laptop computers.

2. PHI may be stored on a portable electronic storage device and/or laptop
computer only if it is essential to do so to accomplish the work of the university. The
necessity of storage shall be determined by the University HIPAA Privacy and Contact
Officer. In the event the University HIPAA Privacy and Contact Officer allows such
storage the departmental information technology employee shall make reasonably
feasible arrangements for data encryption, strong passwords, and/or other appropriate
protection.

3. No device, including portable electronic storage devices and laptop
computers, on which PHI is stored may be left unattended unless it is in a secure, locked
environment.

4. In no case may PHI be stored on a personally owned device of any kind.

5. All PHI contained on portable electronic storage devices and/or laptop
computers shall be backed up daily to the university file servers.

6. Any laptop computer that contains PHI must have computer tracking
software installed as determined by the Office of Information Technology. Software
installation must be arranged through the Office of Information Technology.

Regulatory Authority: Final Privacy Rule: 45 CFR §164.503(c)

Related Policies/Procedures:

• Policy Regarding Incidental Uses and Disclosures
• Policy, Providing Information to Family and Friends of Individuals Involved in Care
• Designated Record Sets

History:
Adopted: December 23, 2008
Effective: January 5, 2009