**Subject:** Electronic Data Storage

**Scope:** Faculty, Staff, and Students that Utilize HIT Supported Devices and Network

**Effective Date:** 7/8/2009

**Last Review/Revise Date:** 12/10/2012

**Responsible Department:** Health Information Technology

---

**Policy**

All institutional and confidential data will be stored on a HIT administered or approved server. Unencrypted data stored on any device, including personal hard drives, flash drives, or any other attached storage, is considered unsecured and is forbidden by the policy. In addition, any data that needs to be transported on any external media must be encrypted. HIT will provide information on approved hardware and software solutions that satisfy encryption requirements.

---

**Purpose**

By implementing and maintaining an electronic data storage policy, Health Information Technology (HIT) will be better able to manage disk space, keep backup times acceptable and ensure the protection of confidential patient or hospital information. Data stored on local PCs is considered unprotected and should be limited to non-institutional data.

This policy addresses all methods of physical and electronic storage. This includes but is not limited to personal computers, laptops, tablet computers, Personal Digital Assistant (PDA), removable flash memory, and servers.

---

**Definitions**

Institutional Data: All of the data and records held by the University, in any form or medium, for the administration, operation, or governance of the University or any unit of the University. The MSU Institutional Data Policy can be found here:


Confidential Data: Confidential Data is defined as (i) Institutional Data that could, by itself or in combination with other such Data, be used for identity theft or related crimes, (ii) Institutional Data whose public disclosure is restricted by law, contract, University policy, professional code, or practice within the applicable unit, discipline, or profession, (iii) records of the University’s security measures, and (iv) Institutional Data whose value would be lost or reduced by unauthorized disclosure or by disclosure in advance of the time prescribed for its authorized public release, or whose unauthorized disclosure would otherwise adversely affect the University financially.

Examples of Institutional and Confidential data

- Social security number;
- Credit card number or debit card number;
- Bank account number, automated clearing house number, or electronic funds transfer account number;
- Driver’s license number;
- Name, address, and date of birth;
- Mother's maiden name;
- Student records that are protected by the Family Educational Rights and Privacy Act (FERPA) or the University's Guidelines Governing;
- Privacy and Release of Student Records;
- Protected health information as defined under the Health Insurance Portability and Accountability Act (HIPAA);
- Research data or results prior to publication or the filing of a patent application;
- Information subject to a contractual confidential;
- Security codes, combinations, and passwords.

**Process**

1. HealthTeam Department Heads/Supervisors will conduct periodic risk assessments of the physical security of the workstations within their areas, taking appropriate measures to correct any deficiencies. HIT (Compliance Office?) will provide guidelines for physical security and risk assessment.
   i. Contact the HIT Security Officer or HIPAA Security Officer (PHI) for assistance, if required.

2. HIPAA Security Officer will conduct risk assessments to clinical and research workstations that access PHI to determine possible security issues on at least an annual basis.
   i. Provide recommendations to department heads or supervisors for improving the physical security of workstations and forward irresolvable issues to the HIT Chief Information Officer (CIO) for resolution.
   ii. The HIT CIO will review and provide recommendations regarding electronic security issues that are beyond the scope of the department heads/supervisors, HIT Security Officer or HIPAA Security Officer to resolve.

3. Documentation of a risk assessment will be maintained per HIPAA guidelines.