Subject: Transfer of Sensitive Data

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

Effective Date: 10/1/2007
Last Review/Revise Date: 12/10/2012
Responsible Department: Health Information Technology

Policy
No sensitive or institutional data shall be electronically transmitted via an unsecured method.

This includes, but is not limited to, the transfer or email of Protected Health Information (PHI), Credit Card data (PCI) or any other sensitive data as listed in the University Policy http://eis.msu.edu/sid outside the HIT secure domain. Any email of PHI/sensitive information inside the HT domain (i.e. to another hc.msu.edu recipient) must have a disclaimer statement attached that states:

Purpose
The purpose of this Policy is to establish minimum requirements for the appropriate use of Institutional Data.

Health Information Technology (HIT) needs to protect the security and integrity of MSU’s Institutional Data without hindering its effective and efficient use. To achieve this objective, the best efforts of every member of the HIT user community are required.

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.

Process
Please see MSU’s policy regarding the use and handling of Institutional Data: (http://eis.msu.edu/documents/institutional_data_policy_current.pdf)

For emails containing sensitive data that are sent outside the ht.msu.edu domain, the following disclaimer will be added:

CONFIDENTIALITY NOTICE: This email communication may contain private, confidential, or legally privileged information intended for the sole use of the designated and/or duly authorized recipient(s). If you are not the intended recipient or have received this email in error, please notify the sender immediately by email and permanently delete all copies of this email including all attachments without reading them. If you are the intended recipient, secure the contents in a manner that conforms to all applicable state and/or federal requirements related to privacy and confidentiality of such information.