ETSU

Policy Title: Movement of HPI
Policy Manual Section: Computer Security / Transactions
Policy Number: HIP CST 050 A
Effective Date: April 14, 2003
Date of Approval: November 12, 2014

Review/Revision History:

Reviewed by:	Date:	Revision Number: (i.e. A, B, C)
Operations Committee	11/12/2014	A

APPROVED BY:

Signature: _____

Signature: _____

Policy:

Members of the ETSU workforce that are authorized and assigned to transport PHI, whether in paper or electronic format, are responsible for maintaining the privacy and security of all PHI and EPHI and for following all ETSU policies and procedures related to confidential information, PHI, and ePHI.

Procedure:

1. PHI, regardless of whether in electronic or paper format, is to be removed from ETSU by members of the workforce only when necessary to complete their job duties and only with prior approval from their supervisor.

2. Workforce members are responsible for maintaining the privacy and security of all PHI that they may be transporting, storing, or accessing offsite, including but not limited to the following:

    a. PHI and EPHI.
    b. Computers that contain or access EPHI.
    c. Media that contain EPHI.

3. Even though encrypted, computers and media must be password protected. No workforce member will write down the password and tape it to the device or any other place where a thief or any other person that finds the device may find it. Password protection must comply with HIP CST 005 B System Access Password.

4. All equipment and media containing EPHI must be transported in a secure manner, even though encrypted, such as in a locked computer bag. In no event will a workforce member leave any equipment, media, or paper PHI unattended and unsecured even if encrypted and in a locked container.

5. All workforce members will immediately report any loss, theft, or other compromise of PHI taken or maintained outside ETSU in accordance HIP CST 056 A Report Procedure.

6. Workforce members that transport PHI home to work on must comply with ETSU's Work at Home Policy.

7. The Privacy/Security Officer is responsible for training workforce members on the security of equipment, media, and paper records containing PHI, including threats thereto, and the contents of this policy. This training will include both initial and periodic refresher training with the latter being conducted at least annually. The training records must be maintained for a minimum of six (6) years from the date of the training.