SPH Portable Storage Device Policy

Beginning October 22, 2008, all University of Texas Health Science Center at Houston (UTHSC-H) confidential or sensitive information that is stored or transported on portable media must be encrypted. Portable storage media are to include any device that allows for the removal and transport of computer files, also known as external hard drives and flash drives. This website has been designed to provide you with the most relevant information regarding these changes and how it will impact you.

This policy applies to **all UTHSC-H faculty, staff and recognized university associates who have access to university-owned data and/or computer resources**. This policy specifically addresses encryption solutions for external drives and flash drives. Users are responsible for storing confidential or sensitive data on encrypted portable devices, or by encrypting such files if stored on unencrypted portable devices. Users are responsible for reporting incidences of non-compliance.

All purchased portable storage devices must include **built-in encryption technology** compatible with university encryption standards established in policy by the UTHSC-H Information Security department. Please note that some portable devices have encryption as an "option", but can still operate without encryption. These devices do NOT meet the standard for this policy. The devices recommended below all have built-in required encryption technology which meets the UTHSC-H encryption policy.

Below is a list of links to important documents regarding the Portable Storage Device Policy.

- **UTHSC-H Portable Storage Device Policy**
- **UTHSC-H Policy and Procedure Library**

The list of available products with built-in encryption is rapidly changing every several months. To obtain the latest product to fit your needs, whether it is USB portable media storage device or an external hard drive, please consult with SPH IT Services.