


# COMMONWEALTH OF PENNSYLVANIA DEPARTMENT OF HUMAN SERVICES, INSURANCE AND AGING

## INFORMATION TECHNOLOGY STANDARD

Name Of Standard: <b>Use of Portable Storage Devices and Media Standard</b>	Number: <b>STD-ENSS001</b>
Domain: <b>Security</b>	Category: <b>Desktop</b>
Date Issued: <b>09/14/2005</b>	Issued By Direction Of: 
Date Revised: <b>06/02/2017</b>	Robert Doren, Chief Systems Engineering Section

### Abstract:

The utilization of portable storage devices and removable media is escalating within the Department of Human Services. The portability, small size, transfer speeds, and large storage capacity of these devices and media make them attractive options for a variety of data needs. However, these same features present security risks, which the Department shall address.

### Commonwealth Policy

The Commonwealth has issued a [Policy Regarding Portable Storage Devices and Removable Media](#) document that addresses the use of these devices and media. It is the individual agencies' responsibility to monitor and control the use of such devices and media and train its workforce in proper and acceptable use of them.

### DHS Policy

The Department of Human Services has issued a [Use of Portable Storage Devices and Media](#) Policy document that also addresses the use of these devices and media.

### DHS Data Requirements

In the course of normal business operations, staff at the Department of Human Services (DHS) is responsible for handling a variety of confidential data. IRS-derived financial data (e.g., FTI data), HIPAA-related medical data, Privacy Act protected information and personnel data are just a few examples of such data. DHS is responsible for maintaining the privacy and security of this data.

Internal DHS policies, state laws, the policies of other partner agencies (e.g., the IRS), or federal laws (e.g., HIPAA) may govern staff or business-partner access to confidential data. These requirements may necessitate:

- Strong authentication of the entity requesting the protected data
- Limits on the data, and/or limits on the use of the data
- Using USB storage devices that include at least 256 bit encryption
- Limits on the media on which the data is distributed
- Limits on the media on which the data resides
- Failure to protect this information properly may subject the Department and its staff to possible civil and/or criminal sanctions or other penalties (such as withholding of future data).

Please refer to [H-Net Data Classification Standards](#) for details on the various categories of data maintained by DHS and associated restrictions.

## **General:**

For a variety of reasons some individuals require the use of various portable storage devices and media in the course of performing their normal duties as an employee of the Department of Human Services (DHS). The Department of Human Services currently provides these devices to individuals that have proven that they have a legitimate need for such a device.

This document shall establish the Department standard regarding the acceptable use of these storage devices and media as well as the procedures for approving and monitoring their use.

This document outlines:

- Use of personal devices
- Acceptable use of these devices for data storage
- Acceptable use of these devices for data transport
- Decommissioning/disposal of such devices
- Process for reporting the accidental loss or theft of such devices

This standard does not address the use of Commonwealth purchased computers and the data stored on the internal storage device.

## **Standard:**

### **Personal Devices**

The use of personal storage devices and media (i.e., those not purchased through the Department) of any form for DHS or Commonwealth business is expressly forbidden, unless explicitly authorized. This includes, but is not limited to the following:

- Personal Digital Assistant (PDA) Devices:
  - Cellular phones, including Blackberry devices, and any other computing and communications devices with network connectivity and the capability of operating in different physical locations

- Portable Storage Devices:
  - Flash Media Cards/Drives, USB memory sticks, External Hard disk Drives
- Bluetooth Enabled Devices
- Internal/External CD and DVD Writers
- Floppy Disks / Writeable and rewriteable CD-ROMs and DVD-ROMs
- Notebook / Laptop, Desktop and tablet Computers
- Digital cameras and audio recording devices

Only agency-owned components (e.g., computer, media and software) can be used to process, access and store PII, FTI data.

### **Department Devices**

All devices and media for use by Department staff, Business Partners and Contracted Staff of the Commonwealth shall be approved and purchased through the appropriate Commonwealth commodities contract. The only portable storage/media devices that may be used to store restricted or confidential Commonwealth information are USB drives that utilize at least a 256 bit encryption.

It is the responsibility of the employee's supervisor to ensure that all hardware shall be registered in the Department's Remedy Asset Tracking system.

The allocation and use of a portable storage device is not an entitlement for an employee. There is no requirement that any employee be issued such devices. Therefore an employee's supervisor or Program Office Security Officer may require an employee to return a Commonwealth owned device at any time.

Please refer to the following policies, bulletins, and agreements for details on security considerations and associated restrictions:

- STD-ENSS029 – Mobile Application
- POL-SEC002 – Cryptography Policy
- POL-SEC006 – Media Protection Policy

### **Acceptable Device Usage**

#### **Use of unapproved application(s) installed on device**

Only Department of Human Services approved data or files may be stored upon and/or run from these devices and media in accordance with the license agreement of the software manufacturer and/or Commonwealth Enterprise contract license, for authorized Commonwealth purposes only.

It is prohibited to bypass, modify, or remove security features utilized on these devices.

#### **Acceptable use of these devices for data storage**

An employee's supervisor and Program Office Security Officers are responsible for approving and monitoring the use of Portable Storage Devices to ensure that they are being used for legitimate business purposes.

## **Acceptable use of these devices for data transport**

Users in the possession of portable storage devices containing "restricted" or "confidential" Commonwealth information shall not leave them unattended at any time.

Portable devices shall not be checked in airline luggage systems, with hotel porters, or other unsupervised handling or storage processes. These devices shall remain in the possession of the traveler as hand luggage.

Whenever "restricted" or "confidential" information is written to a floppy disk, magnetic tape, smart card, CD or DVD-ROM or other storage media, the storage media shall be suitably marked with the highest relevant sensitivity classification. When not in use, this media shall be stored in locked safe, locked furniture, or a similarly secured location. Non erasable media containing restricted or confidential information should be physically destroyed by user when the information is no longer of use.

Storing IRS and Health Insurance Portability and Accountability Act (HIPAA) confidential or HIPAA restricted information/data on a Portable Storage Device and media is forbidden.

If any questions remain regarding the use of portable storage device and media contact your supervisor or Program Office Security Officer.

## **Decommissioning of such devices**

In the event an employee leaves DHS, no longer has the need for such a device or has a device that is no longer functional, the device shall be returned to their supervisor. All data shall be removed or destroyed before a device is returned. The employee's supervisor shall then ensure that the device is removed from the employee's record in the Department's Remedy Asset Tracking system.

## **Process for reporting the accidental loss or theft of such devices**

The user shall take care not to lose the device or to allow theft of the device. If the device/media is lost, stolen or otherwise rendered inoperable, the user shall contact their manager immediately. In the event of a lost or stolen device or media the user shall disclose the nature of data/information that was stored on the device at the time of loss or theft at which time the manager will determine if any confidential information was involved.

## **Violations**

Disregard for information security policies, procedures, and standards constitute improper conduct. Such occurrences will be handled in accordance with personnel policy concerning disciplinary action.

## **Exemptions from this Standard:**

There will be no exemptions to this standard.

## **Refresh Schedule:**

All standards and referenced documentation identified in this standard will be subject to review and possible revision annually or upon request by the DHS Information Technology Standards Team.

## Standard Revision Log:

Change Date	Version	Change Description	Author and Organization
09/14/2005	1.0	Initial document	Pete Marion - DTE
09/15/2006	1.1	Reviewed content, update the Department Device section	Pete Marion - DTE
01/08/2007	1.2	Updated Acceptable Storage Devices and Media / Department Devices.	Pete Marion - DTE
04/10/2007	2.0	Updated and Reformatted	Richard Sage - DTE
09/17/2007	2.1	Updated	Thomas Zarb - DTE
06/24/2010	2.2	Reviewed and updated	Thomas Zarb
07/02/2010	2.3	Repaired link to OA	Richard Sage
10/24/2013	2.4	Reviewed and updated	Mathieu Saury
03/26/2015	2.5	Content reviewed, made cosmetic change (DHS to DHS)	Pamela Skelton
06/02/2017	2.6	Annual Revision	John Miknich