



Travis County Technology & Security Policies

Device & Media Controls, Reuse and Disposal Policy

Policy #: TC-ITS-206
Version #: 1.2

Approved By: Paul Hoppingardner, Chief Information Officer
Effective Date: May 30, 2015

Accountability & Responsibility

This policy is governed by the accountability and responsibility section found [here](#).

Purpose

The purpose of this policy is to outline the receipt, movement, and removal of hardware and electronic media that contain electronic protected health information (ePHI) into and out of a facility and movement within a facility.

Policy

It is the responsibility of any workforce member who uses or is required to maintain hardware or electronic media that contains ePHI to comply with this policy.

Procedures:

General

These procedures govern the receipt, removal, and disposal of hardware and electronic media used for storage of ePHI at Travis County, and the movement of these items within or out of a County facility. Electronic media includes, but is not limited to: any electronic computing devices including laptop or desktop computers, PDAs, or any other devices that may be used to store ePHI; and, diskettes, compact disks (CDs), DVDs, tapes, memory sticks and all related types of removable storage devices.

Disposal of Hardware and Electronic Media

1. To ensure the protection of ePHI, all ePHI stored on hardware or electronic media must be destroyed prior to the decommissioning of the hardware or media itself. If the ePHI needs to be retained for future use, a retrievable copy can be made, however this copy must have access authorizations in place (such as password protection, etc.) to prevent unauthorized access to the ePHI.
2. Methods for irreversibly destroying ePHI include hard drive low level formatting, disk wiping, or degaussing. Physical methods of destroying electronic media include shredding, grinding down, puncturing, shattering, or incineration.

Media Reuse

1. Prior to device or media re-use, all ePHI stored on the device or media must be securely removed. Removal may be accomplished by disk wiping or by utilizing a reliable data destruction utility to ensure the data is non-recoverable. Caution: A typical disk reformat is not sufficient to comply with this requirement.
2. If required, a backup copy of the stored ePHI can be made prior to reuse of the media or storage device if the ePHI is needed for future use. If a backup copy is created it must have access authorizations in place (such as password protection, etc.) to prevent unauthorized access to the ePHI.
3. A written record of any reused or redistributed storage device or media must be created. (See Inventory and Accountability section below.)

Inventory and Accountability

1. Each hardware unit within Travis County must be affixed with an asset tag to identify function and location and assist with compliance with access control procedures.
2. Each unit within Travis County must maintain a tracking record of the movements of hardware and used to store ePHI, including the receipt of any new hardware storing ePHI. This record should contain, at a minimum, the name of the person responsible for the item, the location of the item, and any movement of the item.
3. Each unit within Travis County must maintain a tracking record of the movements of electronic media used to store ePHI, including the receipt of any electronic media storing ePHI. Covered components must notify ITS regarding the use of electronic media that contains ePHI. This record should contain, at a minimum, the name of the person responsible for the item, the location of the item, and any movement of the item.

Policy Revision

Version	Purpose/Changes	Editor	Date
1.0	Travis County Information Technology Services Information	Randy Lott	05/30/2015



Travis County Technology & Security Policies

Version	Purpose/Changes	Editor	Date
	Security Policies Creation		
1.1	Merged Disposal Policy (204) and Media Reuse Policy (209) into this policy. Renamed from Hardware and Electronic Media Accountability policy. Addressed electronic media use and tracking in item #3 for any covered components.	ITS Policy Committee	10/06/2016
1.2	Updated name due to new CIO.	Randy Lott	03/19/2018