

# AHS Media Protection Standard

---

**Jack Green**

**10/9/2013**

The purpose of this procedure is to facilitate the implementation of the Vermont Health Connect's security control requirements for the Media Protection (MP-1, MP-2, MP-2(1), MP-3, MP-4, MP-5, MP-5(2), MP-5(4), MP-6, MP-6(1), MP-6(2), MP-6(5), MP-6(6), MP-CMS-1) Controls.

## Revision History

Date	Version	Description	Author
	.99	Procedures received from HI and reviewed by Referentia	
12/21/2009	1.0	DII Procedure	
10/9/2013	3.0	Procedures reviewed and adapted for VHC business processes and security requirements. Incremented rev to 3.0 for consistency	Jack Green

### PURPOSE/STANDARD STATEMENT:

The purpose of this procedure is to facilitate the implementation of the Vermont Health Connect's (VHC) security control requirements for the Media Protection (MP-1, MP-2, MP-2(1), MP-3, MP-4, MP-5, MP-5(2), MP-5(4), MP-6, MP-6(1), MP-6(2), MP-6(5), MP-6(6), MP-CMS-1) Controls.

The information systems covered in this procedure document contain but are not limited to the following:

- VHC website
- VHC Portal
- VHC workstations and mobile phones
- Network Accounts
- E-Mail accounts

### SCOPE

The scope of this standard includes the VHC and its constituent systems only

### STANDARD

#### **Media Access**

1. Only authorized users are permitted access to digital and non-digital media.
2. Assessment of risk must guide the selection of media for storage, transport, backup, etc., and the associated information contained on that media requiring restricted access.
3. Unmarked media must be protected until the media is reviewed and appropriately marked, at which time the commensurate measure will be employed.
4. System Owners (SOs) must document the processes required to ensure media and the information on the media of their information system are protected from unauthorized access.
  - This includes, but is not limited to, backup media such as tapes or disks and non-digital media such as printouts.
5. Only approved VHC removable digital media must be used to store VHC data.
  - The removable digital media must be hardware encrypted if it contains sensitive Personally Identifiable Information (PII), Confidential Business Information (CBI), or Federal Tax information (FTI).
  - VHC-owned USB removable media shall not be connected to any non-VHC information system

6. Media, both digital and non-digital, containing FTI data is marked, inventoried, tracked, and audited.
  - Media marking follows IRS Notice 129-A or IRS Notice 129-B guidelines.
  - Inventory, tracking, and auditing information is protected and recoverable.

## **Media Marking**

1. Information system personnel shall mark human-readable output appropriately in accordance with protection level markings set forth by VHC.
2. A defined list of removable media types may be exempt from marking as long as the exempted items remain within defined controlled areas.
  - Media containing FTI data are always marked.
3. The assessment of risk must guide the selection of media requiring marking.
4. Information system personnel and users shall adhere to the following when marking documents that contain confidentially sensitive information:
  - Mark documents appropriately in accordance with applicable policies and procedures set forth by the VHC so that it is immediately apparent that the confidentially sensitive information must be protected from unauthorized disclosure.
  - Upon creating, handling, or receiving a document containing information requiring marking, the applicable stamp or watermark detailing the highest level of protection level contained in the document must be applied to the top and bottom of the front and back cover and on the first and last page.
    - i. If the last page is not blank, then the stamp must be applied to the blank back cover.
    - ii. All other pages must be annotated with the highest level of classification contained on each page.
    - iii. Pages that contain information not requiring marking should be annotated as "unrestricted".
5. Information system personnel shall affix printed output with cover sheets (developed by the applicable system personnel) if the printed output is not otherwise appropriately marked.
6. Information system personnel and users shall mark digital media and cover sheets with the following:
  - I. Distribution limitations.
  - II. Handling caveats of the information.
  - III. Applicable security markings, if applicable.
  - IV. "Unrestricted" information or information of low confidentiality does not require marking but may be marked at the discretion of the System Owner (SO) or Information Owner (IO).
7. Media must be marked to the most restrictive protection level of the information contained on the media.

## Media Storage

1. All digital and non-digital media must be physically controlled and securely stored within defined controlled areas using defined security measures.
  - PII and FTI data is encrypted with an approved method of cryptography while at rest.
2. The assessment of risk must guide the selection of media and associated information contained on that media requiring physical protection.
3. "Restricted" and "protected" information stored by VHC personnel and contractors must be physically controlled, and safeguarded in the manner prescribed for the highest classification level of the information contained on the media until the media is sanitized or destroyed.
4. Information system media must be protected until the media are destroyed or sanitized using approved equipment, techniques, and procedures.
5. Archived data must be retained for a minimum of two years, but may be retained for up to seven years.
  - Upon reaching the seven-year timeframe for archived digital and non-digital media, the media is automatically released to the SO for disposition in accordance with record retention schedules related to the information or information system.

## Media Transport

1. All digital and non-digital media must be protected and controlled during transport outside of controlled areas using defined security measures (i.e., locked container, cryptography).
2. Accountability for information system media must be maintained during transport outside of controlled areas using defined security measures (i.e., locked container, cryptography) that are agency-approved, FIPS 140-2 validated or compliant encryption technologies.
3. Activities associated with transport of information system media must be restricted to authorized personnel.
4. All FTI data is transmitted following the VHC FTI Transmission policies.
  - Located at <http://dvha-intra.ahs.state.vt.us/policies-protocols/InfoSec>

## Media Sanitization

1. All information system media (both digital and non-digital) must be sanitized by using approved equipment, techniques, and procedures prior to disposal, release out of organizational control, or release for reuse.
  - All electronic information and licensed software must be removed when disposing of computers with hard drives. IT resources and digital storage media must be cleaned of all information.

- i. The VHC will sanitize all hard drives with a NSA approved sanitization tool for reuse. If, media is not to be reused then it will be destroyed in accordance with IRS pub. 1075.
2. Sanitization mechanisms with the strength and integrity commensurate with the classification or sensitivity of the information must be employed.
3. When handling confidentially sensitive information, VHC shall consult the appropriate IT and programmatic-related records management schedules to determine if and when the information should be destroyed.
4. Media destruction and disposal must be:
  - Performed in an environmentally approved manner.
  - Undertaken when the information is no longer needed in accordance with requirements set forth by VHC, SO, and IO.
  - Accomplished in a safe and effective manner, especially when physically destroying nonmagnetic (i.e., optical) media (e.g., CDs, DVDs).
  - Addressed in the System Security Plan (SSP).
5. Media sanitization and disposal actions must be tracked, documented, and verified.
6. A log must be created and retained for all media destroyed.
7. Standard Operating Procedures (SOPs) for media sanitization must be developed.
8. Users must be trained on these SOPs.
9. The SOP for media sanitization must include steps to document the following information:
  - Report date.
  - Sanitization completion date.
  - Media being sanitized (including serial number or other uniquely identifiable characteristic, if applicable).
  - Party performing sanitization.
  - Sanitization method employed.
  - Sanitization equipment and procedures must be tested quarterly to verify correct performance.
10. Portable, removable storage devices (e.g., thumb drives, flash drives, and external storage devices) must be sanitized prior to connecting such devices to the information system.

#### IMPORTANT INFORMATION

These procedures can be found at <http://dvha-intra.ahs.state.vt.us/policies-protocols/InfoSec>