VERMONT
AGENCY OF HUMAN SERVICES

State of Vermont
Agency of Human Services (AHS)

Policy Title: Information Security Media Protection and Data Sanitization Policy	**Policy No. 5.20** **Revision History Date:** Replaces: VHC-POL-MP Current version: 03/01/20
Attachments/Related Documents:	**Version Number:** 1.0
Name/Title of Authorizing Signature:	**Origination Date:**
☐**Trauma Informed Review**	

Authorizing Signature:  **Effective Date:** 10-21-20

POLICY STATEMENT:

To establish high-level requirements, organizational responsibilities, and managerial commitment for an Information Security Media Protection and Data Sanitization Policy that ensures the confidentiality, integrity, and availability of information and systems within the Agency of Human Services (AHS) in compliance with all applicable State and Federal Law, regulations, or policies, such as those established by CMS, Internal Revenue Service, Social Security Administration, Criminal Justice Information Services, and Vermont law.

BACKGROUND:

HIPAA Physical Safeguards require AHS to: 1) implement technical policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility (45 CFR § 164.310(d)(1)); and2) address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored (45 CFR § 164.310(d)(2)).

This policy also follows the NIST SP 800-53 framework regarding Media Protection. The purpose of this policy is to ensure information system media is properly secured, stored, labeled, and disposed of. The level of security required for information system media is dependent on the security category of the information residing on the information system.

This policy details how AHS complies with Federal information security standards for implementing and maintaining an information Security Media Protection and Data Sanitization Policy.

SCOPE:

This policy governs Information Security protocols related to Media Protection and Data Sanitization and implementation of associated standards and procedures.

ROLES AND RESPONSIBILITES:

AHS Secretary – Responsible for making a final review and approval of this policy.
AHS Policy Committee - Responsible for making a final review of this policy.
Chief Information Security Officer – Responsible for reviewing and approving this policy prior to AHS Policy Committee. The CISO will report all compliance-related activities pertaining to this policy to AHS Secretary.
Authorizing Official - responsible for operating an information system authorized pursuant to AHS Policy 5.08 at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individual's data.
AHS Information Security Director – responsible for:

- creating procedures and standards to meet the requirements established in this policy.
- reporting all matters pertaining to the AHS's compliance with this policy to the CISO and the Authorizing Official; and
- ensuring that this policy is reviewed and updated (if necessary) at least annually.

PROTOCOLS:

This policy covers information stored on digital media which includes, but is not limited to:

- Computer hard drives (HDDs) or Solid-State Drives (SSDs)
- Databases or file servers
- CD/DVD/Blu-ray
- Thumb drives / Flash Media
- SD or data cards
- Cell phone storage or SIM cards

This policy also covers non-digital media such as:

- Reference books and manuals
- Printed documents such as printed emails, office files, etc.
- Images or photocopies

The AHS Information Security Director will establish associated security standards and procedures to meet the following security media protection and data sanitization requirements.

Media Access

Access to digital and non-digital media containing sensitive information will be restricted to authorized roles/departments. Automated mechanisms will be used to control access to authorized individuals only, for areas where media is stored.

Media Marking and Labeling

Media will be labeled or marked to indicate any distribution limitations, handling warnings, and applicable security markings of the data. Any media containing FTI will be marked to indicate "Federal Tax Information." Certain types of approved media or hardware components can be exempt from marking if the media remains within a secure environment.

Media Storage

Physical media will be securely stored within physically protected areas. Digital media will be protected using a FIPS 140-2 validated encryption module. Non-digital media will be protected by locked cabinets or safes. Information system media will be protected until the media is properly destroyed or sanitized.

Media Transport

Protection mechanisms will be used when transporting both digital and non-digital media containing sensitive data outside of controlled areas. Cryptographic mechanisms will be used to protect the confidentiality and integrity of data stored on digital media during transport outside of controlled areas. Backups will be created prior to the movement of equipment or media to ensure availability.

The transportation of media will be limited to authorized personnel only. Accountability of transported media outside of controlled areas will be maintained. All media transportation activities will be documented.

Media Sanitization

All digital and non-digital information system media will be sanitized prior to disposal, release out of organizational control, or release for reuse. All computer desktops, laptops, hard drives, and portable media will be processed for proper sanitization. All media sanitization and disposal action will be reviewed, approved, tracked, documented, and verified. Media sanitization procedures will be implemented to ensure that:

- Sensitive information (such as Electronic Protected Health Information (ePHI) as defined by HIPAA, Federal Tax Information (FTI) as defined by the IRS, or other forms of electronic confidential data) is rendered unusable, inaccessible, and unable to be reconstructed before assets are repurposed.
- Specific technology (e.g. software, special hardware, etc.) mechanisms will be identified to ensure sensitive information is unusable, inaccessible, and unable to be reconstructed.
- Only authorized officials will be permitted to sanitize sensitive information or equipment. Sanitization mechanisms will be employed with the strength and integrity commensurate with the security category or classification of the information.
- Media sanitization procedures and equipment will be tested annually to verify that all media is sanitized properly.

Audit and Management

Documented procedures and evidence of sanitization practices will be obtained and maintained in accordance with applicable legal/regulatory requirements, obligations from business associate agreements, or other internal policies or procedures that dictate record retention. An inventory and disposition records for information system media will be maintained to ensure control and accountability of sensitive information. These records will contain sufficient information to reconstruct the data in the event of a breach.

Media Use

The use of personally owned media on AHS information systems or system components will be prohibited unless permitted under the AHS Personal Equipment Software, and Data Policy number 5.10.

ENFORCEMENT:

The AHS Secretary may initiate reviews, assessments, or other means to ensure that policies, guidelines or standards are being followed.

AUTHORITIES:

- Health Insurance Portability and Accountability Act (HIPAA) Security Rule: 45 CFR Part 160 and Subparts A and C of Part 164
- Centers for Medicare and Medicaid Services (CMS), Minimum Acceptable Risk Standards for Exchanges (MARS-E), Version 2.0, November 10, 2015
- IRS Publication 1075 (Rev. 11-2016)
- Social Security Administration (SSA), *Electronic Information Exchange Security Requirements and Procedures For State and Local Agencies Exchanging Electronic Information With The Social Security Administration* based on: Federal Information Security Management Act (FISMA), Public Law (P.L.) 107-347, the Privacy Act of 1974 and SSA's own policies, procedures and directives
- Criminal Justice Information Services (CJIS), Security Policy, Version 5.7, 08/16/2018, CJSD-ITS-DOC-08140-5.7

REFERENCES:

MARS-E	IRS Pub 1075	SSA	HIPAA	CJIS
MP-1 MP-2 MP-3 MP-4 MP-5 MP-5 (4) MP-6 MP-6 (1) MP-6 (2) MP-7	9.3.10.1 9.3.10.2 9.3.10.3 9.3.10.4 9.3.10.5 9.3.10.6	5.8	§164.310(d)(1) §164.310(d)(2)(i) §164.310(d)(2)(ii) §164.310(d)(2)(iii)	5.8

MP-7 (1) MP-CMS-1				

(Version numbering instructions: Major revisions are reflected in whole numbers, minor or no revisions in tenths.)

Document Version Control			
Version Number	**Version Effective Date**	**Author**	**Description**
1.0		Emily Wivell	Initial Version

APPENDIX:

None.