

DOCUMENT: Policy	DOCUMENT NUMBER: IT-0517	REVISION: Original	PAGE 1 OF 5
SUBJECT: Media Disposal		EFFECTIVE DATE Draft: 02/1705	
OFFICE OF MIS:		DATE:	
SECRETARY OF DHHR:		DATE:	

1.0 PURPOSE

The disposal of media, computer equipment, and computer software can create information security risks. These risks are related to the potential unauthorized disclosure of electronic Protected Health Information (e-PHI) or other sensitive data, violations of software license agreements, and unauthorized disclosure of intellectual property that could be stored in hard disks and other storage media.

This policy will govern the requirements of secure disposal of media containing sensitive data or e-PHI, by establishing a process through which the secure removal of sensitive data or e-PHI is achieved on all media used within the Department of Health and Human Resources (DHHR) prior to disposal.

2.0 SCOPE

This policy applies to all DHHR employees who authorize the disposal, handle the media or devices intended for disposal, or who are directly responsible for the disposal of media and devices containing sensitive data or e-PHI.

This policy covers all fixed and removable storage devices owned by the DHHR. This includes, but is not limited to: magnetic media (including fixed disks, magnetic tape, floppy, and other removable drive disks), optical disks, non-volatile memory devices (including memory sticks and cards or USB memory storage), and PDAs.

Any storage devices currently available, or that become available in the future due to new technology, are also covered by this policy.

3.0 APPLICABLE DOCUMENTS/MATERIALS

- 3.1 Office of Management Information Services (OMIS) Operating Procedure (OP) - 17 - *Media Controls*
- 3.2 DHHR Policy Memorandum 2104, *Progressive Discipline*
- 3.3 DHHR Policy Memorandum 2108, *Employee Conduct*

DOCUMENT: Policy	DOCUMENT NUMBER: IT-0517	REVISION: Original	PAGE 2 OF 5
SUBJECT: Media Disposal		EFFECTIVE DATE Draft: 02/17/05	

4.0 RESPONSIBILITY/REQUIREMENTS

4.1 Disposal/Sanitation Methods (See OP-17, *Media Controls*)

- 4.1.1 OMIS will prescribe a comprehensive data control program for the DHHR.
- 4.1.2 All electronic devices and media equipment, including storage media in personal computers and other hardware containing sensitive data or e-PHI, will be sanitized prior to disposal.
- 4.1.3 The proper sanitation method depends on the type of media and the intended disposition of the media.
 - 4.1.3.1 Media containing sensitive data or e-PHI must be degaussed or destroyed prior to disposal so that data will not be retrieved and re-used.
 - 4.1.3.2 Non-functioning and/or non-writable media containing sensitive data or e-PHI must be physically destroyed if degaussing or other sanitization is determined to be inadequate.
 - 4.1.3.3 Media not containing sensitive data or e-PHI can either be sanitized or destroyed to an appropriate condition.
- 4.1.4 Disposal of media requires authorization and tracking by the data owner of record.
- 4.1.5 All methods of media disposal will be in agreement with information security best practices, while also considering cost-effectiveness and the safety of employees.

4.2 Security Officer Responsibilities

- 4.2.1 The DHHR Security Officer or a designated individual(s) will be responsible for assuring that e-PHI, as well as the hardware or electronic media on which it is stored, is properly destroyed and cannot be re-created.
- 4.2.2 The DHHR Security Officer or a designated individual(s) will oversee the monitoring process.

DOCUMENT: Policy	DOCUMENT NUMBER: IT-0517	REVISION: Original	PAGE 3 OF 5
SUBJECT: Media Disposal		EFFECTIVE DATE Draft: 02/17/05	

4.2.3 The Security Officer or a designated individual(s) will document disposal information beginning with the point of designation for destruction to final disposal.

4.2.3.1 The chain of custody of the data will be established and maintained in the disposal documentation and will clearly identify the asset or media to be disposed, as well as the individual(s) responsible for its disposal.

4.2.3.2 Disposal information will be kept for a period to be specified by the DHHR.

4.3 Policy and Operating Procedure (OP) Updates

4.3.1 Updates to Information Technology (IT) policies and OPs concerning Media Controls will be made on a periodic basis.

4.3.2 All employees responsible for disposal activities will receive periodic training on IT policies and procedures on the use of software and tools utilized to prepare and audit media and devices for disposal.

4.3.3 Disposal activities will be audited on a regular basis by a designated individual(s) in OMIS to verify compliance with IT policies.

4.4 Enforcement Authority

4.4.1 The Information Security Officer (ISO) is the person designated by the Chief Technology Officer (CTO) to monitor and provide initial enforcement of the DHHR's information security program and IT policies.

4.4.2 The Information Security Liaison's (ISL) are employees assigned by the commissioner with each Bureau and/or Office to assist the ISO in the protection of information resources.

4.4.3 The Office of the Inspector General (OIG) is the authority who investigates reported instances of Departmental employee misconduct.

4.5 Violations and Disciplinary Action(s)

DOCUMENT: Policy	DOCUMENT NUMBER: IT-0517	REVISION: Original	PAGE 4 OF 5
SUBJECT: Media Disposal		EFFECTIVE DATE Draft: 02/17/05	

- 4.5.1 All suspected violations of this policy will be reported to a supervisor in the chain of command above the employee.
- 4.5.2 The supervisor or designee will review the facts and, if it is suspected that a violation may have occurred, the matter will be referred to the Office Director or Bureau Commissioner for appropriate action.
- 4.5.3 As determined by the Office Director or Bureau Commissioner, instances of abuse or misconduct, depending on the circumstances, will be referred to either the ISO or the OIG for further investigation.
- 4.5.4 Employees or systems administrators or managers who willfully or knowingly violate or otherwise abuse the provisions to this policy may be subject to: (1) disciplinary action as outlined in DHHR Policy Memorandum 2104; or (2) criminal prosecution.

5.0 DEFINITIONS

- 5.1 Degauss – To demagnetize data from storage devices in order to destroy the media so it is no longer usable.
- 5.2 Device – Including but not limited to personal computers, laptops, handheld units (PDA's).
- 5.3 Disposal - The final disposition of electronic data, and/or the hardware on which electronic data is stored.
- 5.4 Electronic Protected Health Information (e-PHI) – Health information transmitted by or maintained in electronic media used to identify an individual, which is created, used, or disclosed in the course of providing health care services such as diagnosis or treatment. Examples include: names, phone numbers, medical record numbers, photos, etc.
- 5.5 Employee - Individuals employed on a temporary or permanent basis by the DHHR; as well as contractors, contractor's employees, volunteers, and individuals who are determined by the Bureau or Office to be subject to this policy. For the purpose of this policy, this also refers to anyone using a computer connected to the DHHR network.
- 5.6 Media Controls - Formal, documented, policies and procedures that govern the receipt and removal of hardware/software (for example, diskettes, tapes) into and out of a facility.

DOCUMENT: Policy	DOCUMENT NUMBER: IT-0517	REVISION: Original	PAGE 5 OF 5
SUBJECT: Media Disposal		EFFECTIVE DATE Draft: 02/17/05	

5.7 Office of Management Information Services (OMIS) – This office reports directly to the DHHR Deputy Secretary for Administration and provides the leadership, innovation, and services needed to achieve efficient and effective technology solutions to meet the goals of the DHHR.

5.8 Sanitization - The process of rendering data harmless.