

Process

Title:	ODHS OHA 090-011-01 Media Disposal Process
Related to:	ODHS OHA 090-011 Media Protection and Disposal Policy
Effective date:	08/02/2021

Purpose

This process outlines the necessary steps to properly dispose of protected information stored on physical or digital maintained by the Oregon Department of Human Services (ODHS) and the Oregon Health Authority (OHA). Protected information includes personally identifiable information (PII), protected health information (PHI), federal tax information (FTI), Criminal Justice Information (CJI), Social Security Administration (SSA) information, Payment Card Industry (PCI) information, and data covered by 42 Code of Federal Regulations (CFR) Part 2.

Applicability

This process applies to all ODHS|OHA staff including employees, volunteers, trainees, interns, as well as partners and contractors.

As keepers of the public trust, all agency employees have a responsibility to comply with state and agency policies, administrative rules, and state and federal laws. The agency takes this responsibility seriously and failure to fulfill this responsibility is not treated lightly. Employees who fail to comply with state or agency policy, administrative rule, or state and federal law may face progressive discipline, up to and including dismissal from state service.

Process

1. Physical media refers to media in printed form including printed documents, printed imagery, printed facsimile.
2. Digital media includes any form of electronic media designed to store data in a digital format. This includes but is not limited to memory device in laptops, computers, and mobile devices; and any removable, transportable electronic media, such as magnetic tape or disk, optical disk, flash drives, external hard drives, or digital memory card.
3. Protected information is stored on physical or digital media for as minimal amount of time necessary to achieve the intended use of the data. After the physical or digital media containing protected information is no longer needed it must be removed from service and either sanitized for reuse or destroyed.
4. While waiting for sanitization or destruction, physical or digital media are securely stored within physically secure locations or controlled areas, with access restricted to authorized staff.
 - a. When handling media that mixes data types, the most stringent requirement for storage is applied.

- b. ODHS|OHA programs seek guidance from the Information Security and Privacy Office (ISPO) to classify their data according to the level of sensitivity.
- 5. The most stringent requirement for destruction applicable is used in cases where media includes more than one type of protected data.
- 6. The ODHS|OHA staff verify that physical media is destroyed by the following methods based on the type of protected information:
 - a. Shredded on-site by ODHS|OHA staff authorized to handle such information:
 - A. Physical media containing FTI is shredded using cross-cut shredders, rendering the media 0.04-inch x 0.2-inch (1-millimeter x 5- millimeter) in size (or smaller), or pulverized/disintegrated using disintegrator devices equipped with a 3/32-inch (2.4-millimeter) security screen.
 - B. Physical media containing CJI is shredded by Criminal Justice Information Services (CJIS) authorized staff using cross-cut shredders.
 - C. All other physical media including PHI and SSA is shredded using any ODHS|OHA issued shredders.
 - b. Shredded on-site by a contracted entity:
 - A. Physical media containing FTI is shredded using cross-cut shredders, rendering the media 1-millimeter x 5-millimeter (0.04-inch x 0.2- inch) in size (or smaller), or pulverize/disintegrate paper materials using disintegrator devices equipped with a 3/32-inch (2.4-millimeter) security screen, and witnessed by authorized staff throughout the process.
 - B. Physical media containing CJI is shredded using cross-cut shredders and witnessed by CJIS-authorized staff throughout the process.
 - C. Physical media containing PHI shredded by a contracted entity who has a business associate agreement (BAA) with ODHS|OHA.
 - D. All other physical media is shredded to render protected information unreadable.
 - c. Shredded or incinerated off-site by a contracted entity:
 - A. Physical media containing FTI is destroyed by a contracted entity through incineration or shredded as noted in section 4(a)(A) above. This process is witnessed by authorized staff.
 - B. Physical media containing CJI is destroyed by incineration or shredded using cross-cut shredders and completed by a CJIS-authorized contracted entity. This process is witnessed by CJIS-authorized staff throughout the process.
 - C. Physical media containing PHI shredded or incinerated off-site by a contracted entity who has a BAA with ODHS|OHA.
 - D. All other physical media is shredded to render protected information unreadable.
- 7. Staff verify digital media that has processed, stored, or transmitted protected information is disposed of or sanitized based on the type of protected information:
 - a. Digital media containing FTI uses one of the following sanitization techniques which are witnessed or verified by an agency employee:
 - A. If the media is reused for the same purpose of storing FTI and not leaving the agency's control, then clearing¹ is be used as the method of sanitization.
 - B. If the media is be reused and repurposed for a non-FTI function or leaving the agency's control, then purging¹ is be used as the sanitization method.

¹ Refer to Internal Revenue Service (IRS) Publication 1075 Media Sanitization Techniques

¹ Refer to Internal Revenue Service (IRS) Publication 1075 Media Sanitization Techniques

- C. A representative sampling of media is tested after sanitization has been completed. As required by Publication 1075, Section 8.3, every third piece of physical electronic media is checked to ensure appropriate destruction of FTI.
- D. If the media is not reused at all, then the media is destroyed by an authorized contracted entity and witnessed by authorized staff throughout the process.
- b. Digital media containing CJI:
 - A. If the media is reused or repurposed for a non-CJI function or leaving the agency's control, CJIS-authorized staff sanitize the media by overwriting at least three times or degaussing the media (magnetically erasing the data).
 - B. If the media not reused, it is shredded on-site by a CJIS-authorized contracted entity and witnessed by CJIS-authorized staff throughout the process.
- c. For media containing other protected information:
 - A. If the media is reused or leaves the agency's control, media is sanitized by overwriting at least three times or degauss the media.
 - B. If the media is not reused at all, then the media is shredded by authorized staff onsite or offsite by a contracted entity.
- 8. OIS staff maintain records documenting all digital media disposal activities in compliance with ODHS|OHA 010-018 and litigation hold requirements. Documentation includes:
 - a. Information about the media (type, serial number, other unique identifiers).
 - b. The date the media was sanitized, purged, or disposed.
 - c. The person performing the activity.
 - d. The method used to render all data unusable (e.g. software tool used or physical destruction of the media).
 - e. The signature of the person responsible for ensuring that all data on the storage media has been rendered unusable.

References

- [42 CFR Part 2 Confidentiality of Substance Use Disorder Patient Records](#)
 - [45 CFR 160.103 Public Welfare General Administrative Requirements: Definitions](#)
 - [45 CFR 164.310 Physical Safeguards](#)
 - [ORS 279 Public Contracting](#) and [279A Public Contracting](#)
 - [OAR 166-005 Archives](#)
 - [OAR 166-030 Archives and Record Retention](#)
 - [DAS Electronic Waste \(E-Waste\) Overview-Information about E-Waste Recycling, Destruction, and Re-Use](#)
 - [DAS E-Waste Guidelines](#)
 - [DAS 107-011-050 PR Sustainable Acquisition and Disposal of Electronic Equipment \(e-waste/recovery\)](#)
 - [ODHS|OHA 090-011-01 Media Disposal Process](#)
 - [ODHS|OHA 090-011-02 Media Disposal Process Map-Criminal Justice Information \(CJI\)](#)
 - [ODHS|OHA 090-011-03 Media Disposal Process Map-Federal Tax Information \(FTI\)](#)
 - [ODHS|OHA 090-011-04 Media Disposal Process Map-Protected Information](#)
-

[Federal Bureau of Investigation \(FBI\) Criminal Justice Information Services \(CJIS\) Security Policy](#)
[FBI CJIS Security and Management Control Outsourcing Standard for Non-Channelers](#)
[Federal Information Processing Standards Publication \(FIPS\) Standards for Security Categorization of Federal Information and Information Systems](#)
[Internal Revenue Service Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies](#)
[MARS-E Document Suite, Version 2.0, Volume III: Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges](#)
[National Security Agency \(NSA\) |Central Security Service \(CSS\) Media Destruction Guidance](#)
[National Institute of Standards and Technology \(NIST\) SP 800-53 Rev. 5, Security and Privacy Controls for Federal Information Systems and Organizations](#)
[NIST SP 800-60 Volume II, Rev. 1: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories](#)
[NIST SP 800-88, Rev. 1 Guidelines for Media Sanitization](#)
[Payment Card Industry Security Standards Council](#)
[Social Security Administration Information Exchange Security Requirements and Procedures](#)
[Statewide Information and Cyber Security Standards 2019](#)

Related policies

[DAS 50.050.01 Working Remotely](#)
[DAS 107-001-020 Public Records Management](#)
[DAS 107-004-050 Information Asset Classification](#)
[DAS 107-004-051 Controlling Portable and Removable Storage Devices](#)
[DAS 107-004-100 Transporting Information Assets](#)
[DAS 107-004-110 Acceptable Use of State Information Assets](#)
[DAS 107-011-140 Sustainable Procurement and Internal Operations](#)
[ODHS 100-013 Policy on the Business Associate Relationship between ODHS and OHA](#)
[OHA 100-013 OHA Business Associate Relationships](#)
[OHA 010-018 Policy on Records Retention and Management Structure](#)
[ODHS|OHA 010-018 Records Retention and Management Policy](#)
[ODHS|OHA 070-014 Information Technology Asset Management Policy](#)
[ODHS|OHA 090-009 Administrative, Technical and Physical Safeguards Policy](#)

Contact

Information Security and Privacy Office
Security: 503-945-6812
Fax: 503-947-5396
Dhsinfo.security@dhsaha.state.or.us

History

Version 1 ODHS|OHA established 08/02/2021

Keywords

CJI, CJIS, Criminal Justice Information, Criminal Justice Information Services, digital, disposal, dispose, disposition, electronic media, electronic waste, e-waste, federal tax information, FTI, Internal Revenue Service, IRS, media, overwriting, payment card information, PCI, physical media, physical waste, protected information, protection, purging, remote, removable media, rewriteable media, sanitization, shredding, transport, waste

This document can be provided upon request in an alternate format for individuals with disabilities or in a language other than English for people with limited English skills. To request this document in another format or language, contact the Publications and Design Section at 503-378-3486, 7-1-1 for TTY, or email dhs-oha.publicationrequest@state.or.us.