Department of Veterans Affairs
Washington, DC 20420

VA Directive 6371
Transmittal Sheet
May 2, 2008

DESTRUCTION OF TEMPORARY PAPER RECORDS

1. REASON FOR ISSUE: To issue policy requirements for the Department of Veterans Affairs (VA) on the destruction of temporary paper records.

2. SUMMARY OF CONTENTS/MAJOR CHANGES: Numerous measures are being implemented to increase the security and protection of paper records.

3. RESPONSIBLE OFFICE: The Office of Information Protection and Risk Management, Records Management Service (005R1B), is responsible for the material contained in this directive.

4. RELATED HANDBOOK: None

5. RESCISSION: None.

Certified By:

/s/
Robert T. Howard
Assistant Secretary for
Information and Technology

BY DIRECTION OF THE SECRETARY OF VETERANS AFFAIRS

/s/
Robert T. Howard
Assistant Secretary for
Information and Technology

Distribution: Electronic

DESTRUCTION OF TEMPORARY PAPER RECORDS

1. PURPOSE AND SCOPE

a. This directive establishes Department of Veterans Affairs (VA) policy to ensure that Personally Identifiable Information (PII) and other sensitive agency information of all individuals, including veterans, dependents and employees contained in paper records is properly disposed of. Documents that are available on the internet or from other public sources are not bound by this new policy. This policy is applicable department-wide to all employees, contractors, and volunteers.

b. The essential aspect of protecting sensitive information is the awareness and individual responsibility of our employees.

2. POLICY

All PII and sensitive information that is contained in paper records under the jurisdiction of the VA will be handled by the most secure, economical, and effective means. VA must especially protect PII. Extraordinary procedures must be used. Sensitive information that is lost, sent to the wrong recipient, or stolen can result in actual or potential identity theft and personal hardship to veterans and their dependents.

3. RESPONSIBILITIES.

All Under Secretaries, Assistant Secretaries, and Other Key Officials are responsible for the following:

a. Communicating this policy to all employees in their organizations;

b. Evaluating the security and privacy awareness activities of each organization, in order to set clear expectations for compliance with security and privacy requirements;

c. Allocating adequate resources to accomplish such compliance;

d. Developing mechanisms for communicating, on an ongoing basis, each workforce member's role and responsibilities specific to data security and privacy policies and practices that will enhance our security and privacy culture.

4. DEFINITION

a. **Permanent records:** As defined in 36 CFR 1220.14 General Definitions, are those records that have been determined by the National Archives and Records Administration (NARA) to have sufficient value to warrant its preservation in the National

Archives of the United States. As such, they may not be destroyed by pulping, shredding, or any other means. Examples of permanent records are original hardcopy documents for research and development projects.

b. **Personally Identifiable Information (PII):** Information about an individual, including, but not limited to, education, financial transactions, medical history, and criminal or employment history, and information which can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, biometric records, including any other personal information which is linked or linkable to an individual.

c. **Sensitive Information:** VA sensitive information is all Department data, on any storage media or in any form or format, which requires protection due to the risk of harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information. The term includes information whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission; proprietary information; records about individuals requiring protection under various confidentiality provisions such as the Privacy Act and the HIPAA Privacy Rule; and information that can be withheld under the Freedom of Information Act. Examples of VA sensitive information include the following: individually-identifiable medical, benefits, and personnel information; financial; budgetary; research; quality assurance; confidential commercial; critical infrastructure; investigation, and law enforcement information; information that is confidential and privileged in litigation such as that which is protected by the deliberative process privilege, attorney work-product privilege, or the attorney-client privilege; and other information which, if released, could result in violation of law or harm or unfairness to any individual or group, or could adversely affect the national interest or the conduct of federal programs.

d. **Temporary records:** As defined in 36 CFR 1220.14 General Definitions, are those records that have been determined by the Archivist of the United States to have insufficient value to warrant preservation by NARA. Temporary records are eligible for destruction by burning, pulping, or shredding. Examples of temporary records would be copies of hardcopy documents for research and development projects.

5. REFERENCES

a. National Institute of Standards and Technology (NIST) 800-88 Guidelines for Media Sanitization.

b. NSA/CSS 02-01, Evaluated Products List for High Security Crosscut Paper Shredders.

c. NSA/CSS 02-02, Evaluated Products List for High Security Disintegrators.

d. 36 CFR 1220.14 Subpart A, General Provisions, General Definitions.

e. 41 CFR Part 101 - 45, Sale, Abandonment, or Destruction of Personal Property.

f. 44 U.S.C. 3302 § 1228.58 Destruction of Temporary Records.

Implementation Procedures

In order to meet this goal, the following procedures will be implemented agency wide:

1. When a determination is made to dispose of any paper record containing PII or sensitive information, National Archives and Records Administration (NARA) rules and the National Institute of Standards and Technology (NIST) 800-88 Guidelines for Media Sanitization will be followed. NARA's rules are not shredder specific, but the rules are nevertheless applicable, in particular where paper records are to be disposed. NIST 800-88 guidelines are shredder specific.

2. Federal agencies are required to follow regulations issued by the Archivist of the United States governing the methods of destroying records (44 U.S.C. 3302 § 1228.5, Destruction of Temporary Records). Only the methods described in this regulation shall be used.

3. Paper records to be disposed of normally must be sold as wastepaper. If the records are restricted because they are national security classified or exempted from disclosure by statute, including the Privacy Act, or regulation, the wastepaper contractor must be required to pulp, macerate, shred, or otherwise definitively destroy the information contained in the records. The destruction of the information must be witnessed either by a Federal employee or, if authorized by the organization that created the records, by a contractor employee. The contract for sale must prohibit the resale of all other paper records for use as records or documents.

4. Records other than paper records (i.e., audio, visual, data tapes, disks, and diskettes) may be salvaged and sold in the same manner and under the same conditions as paper records. All sales must be in accordance with the established procedures for the sale of surplus personal property. (See 41 CFR 101-45, Sale, Abandonment, or Destruction of Personal Property.)

5. If the records cannot be sold advantageously or otherwise salvaged, because they contain PII or other sensitive information, they must be destroyed by burning, pulping, shredding, macerating, or other suitable means. National Security Agency (NSA) specifications for High Security Crosscut Paper Shredders (NSA/CSS 02-01) and High Security Disintegrators (NSA/CSS 02-02) would be applicable.

6. If shredding is chosen as the method of destruction, the following parameters will be applicable. The chosen shredder device must have a crosscutting capability which produces particles that are 1 X 5 millimeters in size or that will pulverize/disintegrate paper material using disintegrator devices with a 3/32 inch security screen. (Reference NSA Disintegrator Evaluated Products List).

7. No PII or sensitive information should ever be placed into a dumpster or similar device that has not been shredded, pulped, or macerated.

8. Temporary records that are collected for destruction must be kept in a secure, non-public area of the facility, until the destruction is actually completed.

9. Contracts let to destroy temporary records should include specific clauses to insure that PII and other sensitive temporary records are protected until they are actually destroyed.