Department of Veterans Affairs
Washington, DC 20420

VA Directive 6371
Transmittal Sheet
April 8, 2014

DESTRUCTION OF TEMPORARY PAPER RECORDS

1. REASON FOR ISSUE: To revise policy requirements for the Department of Veterans Affairs (VA) on the destruction of temporary paper records, and temporary paper records that contain personally identifiable and sensitive information.

2. SUMMARY OF CONTENTS/MAJOR CHANGES: This revision is being implemented to increase the security and protection of personally identifiable information (PII), personal health information (PHI), and VA sensitive information contained in temporary records. Revisions include;

a. Revision of the definitions for interim and final destruction of temporary paper records; certification of destruction, clarification of circumstances requiring interim destruction of temporary paper records; elimination of the requirement that a contractor witnessing interim destruction provide a certification of destruction to the VA organization that created the temporary paper records; and

b. Elimination for the requirement that an information destruction contractor be National Association for Information Destruction (NAID) certified and the establishment of minimum standards instead.

3. RESPONSIBLE OFFICE: The Office of Information and Technology (005), Office of Information Protection and Risk Management (005R), Office of Privacy and Records Management (005R1) is responsible for the material contained in this directive.

4. RELATED HANDBOOK: None

5. RESCISSION: VA Directive 6371, dated October 29, 2010.

CERTIFIED BY:

/s/
Stephen W. Warren
Executive in Charge and
Chief Information Officer, Office of
of Information and Technology

BY DIRECTION OF THE SECRETARY OF VETERANS AFFAIRS

/s/
Stephen W. Warren
Executive in Charge and
Chief Information Officer, Office
of Information and

Technology Distribution: Electronic Only

DESTRUCTION OF TEMPORARY PAPER RECORDS

1. PURPOSE AND SCOPE

Temporary paper records are often the most vulnerable type of media utilized by the VA. VA sensitive data, in particular PII, PHI, and VA sensitive information which is disposed of in unsecured containers, leaves the Department vulnerable to access by unauthorized individuals, such as "dumpster divers" and overcurious employees. This directive establishes VA-wide policy for employees, trainees, volunteers, other appointees, contractors and associates, to ensure that all temporary paper records, in particular those that contain PII, PHI, and VA sensitive information under the jurisdiction of VA, will be handled securely, economically, and effectively and disposed of properly. The essential aspect of protecting sensitive information is the awareness and individual responsibility required by everyone identified in this Directive. This Directive does not apply to temporary paper records that are subject to retention pursuant to the applicable records control schedule or that must be preserved in accordance with a litigation hold or preservation order.

2. POLICY

a. Not all VA data contained in temporary paper records is sensitive, however, sensitive data that is contained in temporary paper records often are PII, PHI, and VA sensitive information. Regardless of whether the temporary paper records contain PII, PHI, or VA sensitive information, they must be handled and disposed of properly. Temporary paper records will be disposed of securely, economically, and effectively in accordance with applicable disposition instructions. Sensitive information that is not disposed of properly could result in harm to the Department and/or to subject individuals. Wherever feasible, temporary records should be recycled, while still meeting the requirements for final destruction. Procedures for the destruction of temporary paper records including those temporary records that contain sensitive information, and the minimum set of standards that information destruction contractors (and their subcontractors or third parties) must meet are contained in Appendix A of this document.

b. The protection of PII, PHI and other VA sensitive information through the awareness of proper privacy, security, and records management practices is the responsibility of every member of the VA workforce.

c. This policy only covers temporary paper records. It does not apply to other temporary records in other physical formats such as microfiche, tapes, patient wristbands, or radiology film or electronic records that contain PII, PHI and/or other VA sensitive information. Each Administration shall review its use of other non-paper temporary records and create, as necessary, their own Directives for their final destruction.

d. This policy does not preclude the Administrations or Staff Offices from issuing their own more stringent destruction policies.

3. RESPONSIBILITIES

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

a. Ensuring that this policy is communicated to all employees in their respective organizations;

b. Monitoring and evaluating, on an on-going basis, the security and privacy practices of their organizations as related to the destruction of temporary paper records and those temporary records that contain sensitive information in order to set clear expectations for compliance with security and privacy requirements sufficient to protect and properly dispose of both types of temporary paper records;

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 the destruction of temporary paper records and how to follow the policies and procedures that will enhance and improve VA's security and privacy culture; and

e. Establishing guidance in support of this Directive. For example, some Administrations may require periodic audits conducted by a party independent of the facility, to assess implementation of this policy.

4. REFERENCES

a. Federal Records Act, 44 U.S.C. Chapter 31.

b. Freedom of Information Act, 5 U.S.C. §552.

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

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

e. OMB Circular No A-130.

f. VA Directive 6300, Records and Information Management.

g. VA Directive 6500, Managing Information Security Risk: VA Information Security Program.

h. VA Directive 6502, VA Enterprise Privacy Program.

i. VA Handbook 6300.1, Records Management Procedures.

j. VA Handbook 6500, Risk Management Frame

k. National Institute of Standards and Technology NIST 800-88 Guidelines for Media Sanitation.

l. 36 CFR 1220.18 Subpart A, General Provisions, General Definitions.

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

n. 44 U.S.C. 3302 § 1228.58 Destruction of Temporary Records. Framework for VA Information Systems – Tier 3: Information Security Program.

5. DEFINITIONS

a. **Certification of Destruction.** Written documentation that attests to the completion of the destruction process after the final destruction, as defined by this policy, of VA temporary paper records have taken place. Certification documentation can be in the form of a letter, memo, or any format attesting to its complete destruction. This certification is not considered a valid certification of destruction if completed and submitted prior to the final destruction of the records. The certification should contain sufficient information to attest to the final destruction of the temporary paper records – what temporary records were destroyed, the date when they were destroyed, what destruction method was used, where they were destroyed, and who was responsible for their final destruction.

(1) If the final destruction is completed by VA, then the written certification of destruction is completed by the VA department or personnel that performed the final destruction

(2) If the final destruction is completed by an information destruction contractor, then the written certification of destruction is completed by the information destruction contractor

(3) If the final destruction is completed by a subcontractor to the information destruction contractor, then the written certification of destruction is completed by this third party or by the information destruction contractor with assurance from the third party that final destruction was completed. If the final destruction is completed by a subcontractor to the information destruction contractor, then the written certification of destruction is completed by this third party or by the information destruction contractor

with assurance from the third party that final destruction was completed. The assurance can be in general terms describing the destruction method, date of destruction and amount destroyed, i.e., 75 bales of shredded material.

b. **Final Destruction.** The process through which temporary paper records are pulped, macerated, shredded or otherwise destroyed to a degree that definitively ensures that they are not readable or reconstructable to any degree. If this final destruction is performed away from a VA facility it must be performed by an information destruction contractor (or its subcontractor of third party) who has demonstrated that:

(1) Its destruction process constitutes final destruction as defined in this Directive; and

(2) It has implemented reasonable physical safeguards to protect VA temporary paper records during their transportation, transfer, or short-term storage prior to the completion of their final destruction. Long-term storage (*e.g.*, more than 30 days) must be approved in advance and in writing by the VA organization that generated the temporary paper records.

c. **Interim Destruction:** Any physical destruction process that substantially reduces the risk that PII, PHI, or other VA sensitive information will be disclosed during transport and short-term storage (*i.e.,* less than 30 days) of temporary paper records but does not meet the requirement of final destruction as defined in this Directive. Interim destruction is a reasonable physical safeguard that affords an additional layer of security for temporary paper records once they are identified for destruction. This may be while they are stored at a VA location awaiting final destruction or when they are removed from VA custody until final destruction is completed at an off-site location. It is generally accomplished through maceration, chopping, pulverization, or shredding where these processes do not render the material unreadable or where the material could be reconstructed. Interim destruction is not required but is strongly recommended to reduce risk; it will be a consideration as to whether a facility has completed due diligence in the event of a data breach.

d**. Permanent records.** As defined in 36 CFR 1220.18 General Definitions, are those records that have been determined by the Archivist of the United States, National Archives and Records Administration (NARA), to have sufficient value to warrant their preservation in the National Archives of the United States. As such, <u>they may not be destroyed</u> by pulping, shredding, or any other means. An example of permanent records are <u>original</u> hardcopy documents for research and development projects.

e. **Protected Health Information (PHI).** This term applies only to individually-identifiable health information that is under the control of VHA, as VA's only Covered Entity under HIPAA. PHI is health (including demographic) data that is transmitted by,

or maintained in, electronic or any other form or medium. PHI excludes employment records held by an employer in its role as employer, records of a person deceased for more than 50 years, and some education records. It includes genetic information.

f**. Personally Identifiable Information (PII).** Any information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. Information does not have to be retrieved by any specific individual or unique identifier (i.e., covered by the Privacy Act) to be personally identifiable information. SOURCE: Office of Management and Budget (OMB) *Memorandum 07-16, Safeguarding Against and Responding to Breaches of Personally Identifiable Information* (May 22, 2007).

g. **Readable.** Printed data is readable when strategies can be used to assist with decoding (the translation of letters and/or into sounds or visual representations of speech) data and arriving at comprehension through the use of morpheme, semantics, syntax, and contextual clues to integrate the information they have read into their existing framework of knowledge in order to arrive at a meaning.

h**. Reconstructable.** Printed data is reconstructable when methods can be employed to reassemble the various portions of material in such a fashion that data can be decoded as to make it readable so that meaning can be derived from the data found on the media.

i. **Records.** As defined in 44 U.S.C. 3301, records are all books, papers, maps, photographs, machine readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of the data in them.

j. **Temporary records.** As defined in 36 CFR 1220.18 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.

k. **VA Sensitive Information:** All Department information and/or 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 not only information that identifies an

individual but also other information whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission; proprietary information; and records about individuals requiring protection under applicable confidentiality provisions. SOURCE: 38 U.S.C. § 5727. For purposes of this Directive, these confidentiality provisions include, but are not limited to the Privacy Act; 38 U.S.C. 5701, 5705, and 7332; the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule; and information that can be withheld under the Freedom of Information Act.

For purposes of this directive, examples of VA sensitive information include: individually-identifiable medical, benefits, and personnel information; financial; budgetary; identifiable research; quality assurance; confidential commercial information; 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.

Implementation Procedures

In order to meet the goal of ensuring the destruction of PII, PHI, and other VA sensitive information in the most secure, economical, and effective means, in accordance with legal requirements, the following procedures will be implemented Department-wide:

1. Federal agencies are required to follow regulations issued by the Archivist of the United States governing the methods of destroying temporary records, (36 C.F.R. 1228.58, Destruction of Temporary Records). Only the methods described in this regulation and policy will be used.

2. Under 36 C.F.R. 1226.24, temporary paper records to be disposed of that do not contain sensitive information must be sold as wastepaper or otherwise salvaged. However, if the temporary paper records require special protection because they are national security classified or deemed confidential by statute (such as the Privacy Act of 1974, 38 U.S.C. 5701, 5705, and 7332, and/or the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, regulation, or VA policy), then VA or its information destruction contractor must burn, pulp, shred, macerate or otherwise definitively destroy the information contained in the temporary paper records so that it is not readable or reconstructable to any degree.

3. The destruction of national security classified information, including the method of destruction, must be approved by the VA Security Officer, Office of the Assistant Secretary for Operations, and Security and Preparedness. NOTE: Generally, regular Administration operations do not produce national security classified information.

4. Before the method of destruction is decided, the organization must consider the following, among other factors:

a. What types of information does the organization require to be destroyed?

b. What is the sensitivity of the data?

c. Will the temporary paper records be stored in a controlled area until final destruction?

d. Should the destruction process be conducted within VA the organization or outsourced?

e. What is the anticipated volume of temporary paper records to be destroyed?

f. What is the availability of destruction equipment and tools?

g. What is the level of training necessary for personnel to properly use the destruction equipment?

h. How long will destruction take?

i. What are the costs associated with the various methods of destruction?

j. What are the environmental impacts of the various methods of destruction?

5. The contract for sale of temporary paper records that do not contain PII, PHI other VA sensitive information or national security classified information must prohibit the resale of all such temporary paper records for use as records or documents.

6. The interim destruction of temporary paper records is an important physical safeguard for protecting VA sensitive information whenever transportation or short-term storage (*i.e.,* less than 30 days) of temporary paper records is necessary before final destruction. Interim destruction should be done whenever reasonably practicable.

7. If interim destruction is reasonably practicable and is not carried out by VA employees, it must be carried out by either:

a. A National Association for Information Destruction (NAID) certified, bonded, and insured contractor (and its subcontractors or third parties) for paper/printed media destruction who has contracted to provide sufficient reasonable safeguards to protect the temporary paper records until final destruction has been completed; or

b. A non-NAID-certified contractor (and its subcontractors or third parties) who can satisfy the standards outlined in this Appendix.

8. If interim destruction is not reasonably practicable and VA temporary paper records are removed from VA custody for final destruction, then the VA organization that created the temporary paper records must do the following:

a. Create and maintain documentation showing that interim destruction was not reasonably practicable; and

b. Ensure that the information destruction contractor uses sufficient reasonable safeguards to protect the temporary paper records until final destruction has been completed. In addition, the information destruction contractor must, prior to departing the VA location, provide the designated VA representative with documentation that acknowledged receipt of the temporary records.

9. Methods of interim destruction carried out by an information destruction contractor must be witnessed by a VA employee or, if authorized by the VA organization that created the temporary paper records, a contractor (or subcontractor or third party) employee may act as witness. If a contractor (or subcontractor or third party) employee

is the witness, then that individual must, prior to departing the VA location, provide the designated VA representative with documentation that acknowledges receipt of the temporary paper records.

10. Certificates of destruction from information destruction contractors must be maintained in accordance with applicable VA Records Control Schedules, and should be completed and provided to the VA organization that created the temporary paper records only after final destruction has actually taken place. VA personnel responsible for documenting the final destruction of temporary paper records must develop a tracking method for ensuring that a certificate of destruction is submitted for every shipment of temporary paper records released to an information destruction contractor.

11. Although lesser destruction measures (*e.g.,* interim destruction) may be taken prior to the secure transport of temporary paper records, final destruction of the records must ensure that the information on the temporary paper record is not readable or reconstructable to any degree. If final destruction is not carried out by VA employees, then the final destruction must be witnessed by a VA employee or, if authorized by the VA organization that created the temporary paper records, a contractor (or subcontractor or third party) employee may serve as witness. If final destruction is not carried out by VA employees, it must be carried out by either:

a. A NAID certified, bonded, and insured contractor (and its subcontractors or third parties) for paper/printed media destruction; or

b. A non-NAID-certified contractor (and its subcontractors or third parties) who can satisfy the standards outlined in this Appendix.

12. If the final destruction is witnessed by a contractor (or subcontractor or third party), then the contractor must submit a valid certificate of final destruction to the VA organization that created the temporary paper records.

13. Temporary paper records that are collected for destruction must be kept in a manner that will prevent their content from being read by individuals with no official business need or right to access the data contained in them. The method of collecting and processing these temporary paper records must also prevent their loss or theft until their final destruction.

14. Contracts for information destruction services must be in writing and in accordance with VA and Federal acquisition requirements. Acceptance of a contract for the destruction of temporary paper records must not be through the use of purchase cards or other informal means. Acceptance must be via a fully-executed and current written contract. Payment for contracted services, however, may be made with a purchase card once a fully executed and current contract is in place and the contract number is entered onto the purchase card order.

15. All mandatory VA Acquisition Regulation (VAAR) and Federal Acquisition Regulation (FAR) contracting, security, and privacy clauses must appear in all contracts let for the destruction of VA temporary paper records.

16. Contracts governing the final destruction of temporary paper records containing PII or other VA sensitive information must contain a clause providing for inspection, upon request, by a VA representative, of the contractor's (and subcontractor's or third party's) facilities where the temporary paper records are processed and final destruction takes place.

17. Contracts for destruction of temporary paper records must include specific clauses to ensure that PII and other VA sensitive information is handled and stored in a secure manner until it undergoes final destruction. At a minimum, these contracts shall require documentation that the contractor (or subcontractor or third party) who accepts custody of the temporary paper records from a VA facility and transports them to the final destruction location is either:

a. A NAID certified, bonded, and insured contractor (and its subcontractors or third parties) and can provide reasonable physical safeguards for the temporary paper records throughout the destruction process; or

b. A non-NAID-certified contractor (and its subcontractors or third parties) who can satisfy the standards outlined in the Minimum Standards for Information Destruction listed in this Appendix.

18. If one or more subcontractors (or third parties) handle VA temporary paper records before final destruction, then the contract shall require documentation in any and all subsequent contracts or agreements between the primary information destruction contractor and their subcontractors or third parties that the subcontractors or third parties shall provide sufficient reasonable safeguards for the temporary paper records, to the same standards required of the primary contractor, throughout the destruction process.

19. The assigned Records Manager for the VA organization that created the temporary paper records must review all contracts related to the destruction of temporary paper records to ensure that the requirements of this Directive are satisfied.

20. VA temporary paper records containing PII, PHI, or other VA sensitive information that have not been shredded, pulped, chopped, or macerated to the standard of final destruction shall never be placed with trash, recycling, or other refuse.

21. Collection containers distributed throughout any VA facility must be secured in a manner that prohibits unauthorized individuals from accessing temporary paper records identified for destruction that have been deposited into them. These containers must

provide reasonable physical safeguards which may include, among other measures, locks or placement in secure areas.

22. Veterans Health Administration (VHA) programs and facilities must enter into a fully executed Business Associate Agreement with all information destruction contractors who complete interim and/or final destruction off-site or not under the direct control and monitoring of VHA personnel.

Minimum Standards for Information Destruction

Information destruction contractors and subcontractors must be able to meet the following standards:

1. Physical and Operational Security

a. Monitored Alarm System(s) that include the following:

- Motion Detectors;
- Door Contacts;
- Battery Back-Up; and
- Monitoring Service.

b. Taped Closed Circuit TV (CCTV) monitors with the following:

- Fully Functional Cameras;
- Recording Devices; and
- Secure Recording Tape Library.

c. Sufficient Lighting to allow CCTV

d. Locks and Key Controls

e. Visitor Logs

- Visitor In/Out Logs; and
- Visitor ID Badges.

f. Written Policies and Procedures

2. Documentation and Control of Resources

a. Documentation and control of employees:

- Documentation of who has access to materials (minimum necessary access only is allowed);
- Documentation of background investigations (types and frequency);
- Documentation of citizenship, naturalization (no non-US citizens);
- Documentation of drug screen; and
- Documentation of re-evaluation of above items (at least every two years).

b. Documentation and control of destruction equipment:

- Type (Mobile or Plant-Based);
- Manufacturer and Model;
- Serial Number; and
- Dates of non-operational downtime for repair.

c. Documentation and control of destruction and collection vehicles:

- Vehicle make and model;
- License plate number;
- State/County of registration;
- Acceptable overnight storage address and location;
- Acceptable roadworthiness of vehicles;
- Locks and security of vehicles; and
- Driver logs to show who has control of vehicle at any given time.

d. Documentation and control of all recipients of materials:

- Name of individual/company;
- Address where received;
- Method of final disposition; and
- Certifications of destruction (general documentation acceptable as long as it is attributable to VA's data (*e.g.,* "bails shipped on <date> were pulped on <date>).

Other Operational Requirements

a. All destruction will take place within the enclosure of the destruction facility, which consists of four solid walls and a ceiling, and meets all criteria related to physical building security.

b. The only permissible uses of a mobile destruction vehicle will be within the enclosure of the destruction facility, on-site at the VA's premises, or at an off-site location if approved of in advance by VA and is located within walking distance of the VA premises.

c. A log is kept to record the dates and times that the mobile destruction vehicle is operating within the destruction facility, which shall be made available to VA during an audit, by means of review of CCTV images.

d. The mobile destruction vehicle will be made available to VA for audit, within the enclosure of the destruction facility, during the initial audit and during all scheduled re-audits, for demonstration purposes.