Chapter 5
SENSITIVE ACCESS AND PERSONALLY IDENTIFIABLE INFORMATION

5.01 Introduction

5.02 References and Resources

5.03 Sensitive Access Levels

a. Description of Sensitive Access Levels
b. Authorization for Access to Sensitive Files
c. Deviation from the Policy on Sensitive Access

5.04 Personally Identifiable Information (PII)

a. Definition of PII
b. Policy on the Handling and Storage of VR&E Documents and Claims
c. Permitted Contents of Desk Drawers, Credenzas, Personal Lockable Cabinets, and Other Personal or Provided Storage Containers
d. Employee Accountability in Regard to Disposal of Documents
e. Review Process for Document Destruction
f. Policy on the Handling and Storage of VR&E Documents and Claims when Working from Home
g. Policy on the Handling and Storage of VR&E Documents and Claims When Conducting Off-site and Outreach Activities
h. Handling Veterans' Personal Information Including Mock-up Folders Provided to VR&E Contractors

5.05 Restrictions on Use of Electronic Mail (Email) and Facsimile (Fax) Machine

5.06 Social Media

Appendix O. VA Forms

Appendix V, Rules for Taking Files or Information Off-Site

Appendix AD. VR&E Sign-Out Log

Chapter 5
SENSITIVE ACCESS AND PERSONALLY IDENTIFIABLE INFORMATION

5.01 Introduction

This chapter provides guidelines to ensure that all Department of Veteran Affairs (VA) records are accessed and protected in the proper manner. It also provides procedural guidance for the development, retention, transmission and destruction of personal information by Vocational Rehabilitation and Employment (VR&E) staff and contractors.

5.02 References and Resources

Publications: VA Handbook 6500.6

VA Form (VAF): VA Form 20-8824e, Common Security Services Access Request Form

5.03 Sensitive Access Levels

a. Description of Sensitive Access Levels

Some VA records require additional security measures to ensure that the privacy of the individual is protected. These records are assigned a sensitivity level and corresponding access level, and only employees who have the corresponding level of clearance can access those files. The table below describes this process:

Level of Sensitivity	VA Records Including Employees, Veterans or Their Beneficiaries	Expiration Date	Authorized Employees
9	The President/Vice President of the U.S.; Members of the Cabinet; U.S. Senators and Members of Congress; U.S. Supreme Court Justices; VA Secretary; VA Deputy Secretaries; VA Under Secretaries; VA Asst. Secretaries; other high profile individuals; special cases, e.g. witness protection	Indefinite	Under Secretary for Benefits (USB); Deputy USBs; Service Directors; SIPO Director; Directors and Asst. Directors of facilities having jurisdiction over records with a level of sensitivity equal to 9
8	VA Senior Executive Service; Directors and Assistant Directors; Regional Counsel; Div. Chiefs or equivalent; persons of national prominence; Governors; Lt. Governors; Attorneys General of states or commonwealths; locally prominent persons or officials	3 years after leaving public or government service	Facility Directors and assistants; Area Directors; Veteran Service Center (VSC) Managers and Assistants; all other Division Chiefs

Level of Sensitivity	VA Records Including Employees, Veterans or Their Beneficiaries	Expiration Date	Authorized Employees
7	Veterans Benefit Administration (VBA) employees; private attorney fee cases	3 years after leaving public or government service. The exception is private attorney fee cases. These cases remain level 7 until the Attorney Fee designation for a particular claim no longer exists.	Information Security Officer (ISO) and AISO, System Security Officers, Supervisory Accredited VSO reps; Private Attorneys; all VA Supervisors with a business need; and 10% of a VBA entities' non-supervisory staff with a business need.
6	VA Employees (other than VBA employees); VSO employees, relative of employee; VA work-study/interns employed at a VBA location. At the Director's discretion, this sensitivity level may also be placed on a Veteran's folder for high-profile claims.	3 years after leaving public or government service	Journey level employees having a business need on a daily basis, not to exceed 25% of a VBA entities' non-supervisory staff; non-supervisory accredited VSO reps.
5-0	Local Use Determination		

b. Authorization for Access to Sensitive Files

The Regional Office (RO) Director or Assistant Director is responsible for authorizing access to sensitive files. All sensitive level access requests must

be submitted via Common Security Employee Manager (CSEM), or by using VAF 20-8824e for offices not currently using CSEM. VAF 20-8824e must be submitted to the RO's ISO to request for sensitive level access. See Appendix O, VA Forms, for information on how to access this form, as well as all forms referenced in this chapter.

- Access levels 8 and 9 may be given to employees with designated positions as listed in the chart above.

- Access level 7 restrictions are limited to a maximum of 10 percent of non-supervisory staff allowed access.

- Access level 6 access is limited to an additional 25 percent of non-supervisory staff, with the stipulation that such access is given only to journey level employees. Therefore, a total of 35 percent of RO employees are entitled to Level 6 access and above, to include VR&E employees.

- Access levels 1-5 are not currently in use.

- All other employees should remain at level 0.

c. Deviation from the Policy on Sensitive Access

Due Common Security System (CSS) restrictions, VR&E Divisions, particularly outbased sites, may experience difficulty in managing certain cases, including those that involve access to sensitive files in CWINRS, such as Veteran-employee files, VSC employee files, and work-study student files. In order for VR&E staff to effectively manage a case involving one of these types of files, a request for deviation from the policy on sensitive access levels may be needed.

The VR&E Officer must submit a request, in writing, to the RO Director or Assistant Director for a one-time or temporary deviation from the policy on sensitive access levels. These requests may include access to more than one sensitive file. The RO Director or Assistant Director may provide temporary access to the file at the appropriate access level, and must ensure that the temporary access is rescinded immediately after the necessary action is taken, such as in the event that development is completed and/or the claim is processed, or the Veteran completes or discontinues his/her rehabilitation program. If necessary, the RO Director or Assistant Director may renew sensitive level access requests.

5.04 Personally Identifiable Information (PII)

a. Definition of PII

PII is any information maintained by VA about an individual, such as education, financial transactions, medical history, and criminal or employment history, which can reasonably be used to identify that individual and information which can be used to distinguish or trace an individual's identity.

Examples of PII include, but are not limited to, the following:

- Name, such as full name, maiden name, mother's maiden name, or alias.
- Personal identification number, such as Social Security Number (SSN), passport number, driver's license number, taxpayer identification number, or financial account or credit card number.
- Address information, such as street address or email address.
- Personal characteristics, including photographic image (especially of face or other identifying characteristic), fingerprints, handwriting, or other biometric data (e.g., retina scan, voice signature, facial geometry).
- Any other personal information which is linked or linkable to an individual, such as telephone number, or date and place of birth.

b. Policy on the Handling and Storage of VR&E Documents and Claims

1. VR&E employees with permanent office space are authorized to store Counseling, Evaluation, and Rehabilitation (CER) folders, VR&E or Ed/Voc applications, award related documents, contractor or school invoices, correspondence, and other material related to specific claimants. This information may be stored in the following locations:
    - VR&E Division file bank, sensitive file locked file cabinets, and designated secure file storage locations.
    - File carts and sorting tables in areas that are restricted from Veteran access.
    - Clearly marked holding areas, such as open shelving, tables, or cabinets that are restricted from Veteran access.
    - Unlocked above-the-work-surface storage compartments that are part

of an individual workstation.

- File cabinets specifically provided to employees for the storage of cases under their jurisdiction.

- Desk, on the top of a work site credenza, or other surface clearly visible to supervisory inspection, but not visible during individual counseling sessions.

2. Loose mail or pending award or invoice documents are stored at their individual work site in a clearly marked "Active Mail In-box" on the work surface. However, this information must not be visible during individual counseling sessions.

3. When a case manager is meeting individually with a Veteran, only the Veteran's CER file may be visible on the work surface. All paper records must be stored out of view of the Veteran. The case manager must use privacy screens on computer screens to safeguard electronic information.

4. The VR&E Officer must ensure that all other information is stored in file cabinets or other systems specifically designated. In-boxes or other portable work systems should be located in an area of the VR&E staff member's office that is not visible to the Veteran.

5. The case manager must ensure that a Veteran will not be left unaccompanied in his/her office or any area within the VR&E office. The case manager must also ensure that the Veteran is escorted to and from the designated waiting area.

c. Permitted Contents of Desk Drawers, Credenzas, Personal Lockable Cabinets, and Other Personal or Provided Storage Containers

1. The following items may be stored in the storage containers indicated:

- Personal items

- Office supplies

- Reference materials

2. Under no circumstances will CER folders, VR&E or Ed/Voc applications, subsistence allowance award and related documents, school or contractor invoices, loose mail, or material containing personal identifying information be stored in any of the above referenced containers. Material

being used to develop training courses, such as sample entitlement determinations, must be stored in a lockable cabinet clearly designated for training course material.

3. Personal storage areas may be locked during work hours, but must be unlocked during non-work hours. All work areas are subject to supervisory inspection to ensure proper storage and safeguarding of records. Inspection of work areas will also be conducted during field oversight visits.

d. Employee Accountability in Regard to Disposal of Documents

All VBA employees, contractors, co-located employees of other federal and state agencies, volunteers, and Veterans Service Organization (VSO) staff physically located within facilities under their jurisdiction must comply with VBA policy regarding the disposal of Veterans' records. This policy covers VBA facilities and worksites, regional offices and centers, outbased sites, briefing locations, and approved work-at- home or telecommuting sites.

1. Each employee must be provided a red envelope and box to place material to be shredded. Based on the volume of paper processed by the employees, the appropriate quantity of red envelopes and corrugated storage boxes (6"H x 12"W x 15"L, 10"H x 15"W x 15L or 10"H x 5"W x 24"L or similar sizes) will be purchased by the RO and distributed to employees.

2. Employees must use the red envelopes for claims-related materials only. All red boxes and envelopes will be labeled with the applicable employee's name. The red corrugated boxes are to be reused and will not be destroyed as long as the boxes are in serviceable condition. If a red shred box is deemed unserviceable, it will be replaced immediately. The RO Director is responsible for ensuring that sufficient quantities are readily available to replace unserviceable items.

3. Original copies of legal documents that duplicate records in the Veteran's claims file (birth certificates, marriage certificates, divorce decrees, DD Form 214s, Report of Separation etc.) are not to be destroyed, but returned to the Veteran.

4. Internally generated papers, such as screen or award prints and work papers not appropriate for inclusion in the Veteran's record, do not require signatures, initials, or dating, but must be placed in the employee's red corrugated shred box when submitted for shredding.

5. The following documents require only the employee's signature (or legible initials), before placement in red boxes for shredding:

    - Compensation and Pension Records Interchange (CAPRI) records, which are available electronically if needed for evidence at a later date).

    - Draft or duplicate rating decisions, notification letters, and MAP-D letters.

    - Training materials that include PII.

6. The following claims documents require the employee's signature and the supervisor's signature:

    - Claims and evidentiary submissions deemed duplicates submitted by the Veteran or his/her representative.

    - Waivers, administrative decisions, formal findings, etc., submitted by the Veteran or his/her representative that are determined to be duplicate VA documents of evidentiary nature.

    - Duplicate evidentiary submissions from third parties external to VA.

e. Review Process for Document Destruction

1. Employees will perform the following actions in order to ensure the proper destruction of documents that contain PII:

    - Bundle documents by beneficiary name.

    - Sign, date, and annotate single pages indicating the reason for destruction (e.g., "duplicate record").

    - Bundle and staple multiple pages together, with the top page signed, dated, and annotated with the reason for destruction.

    - Place bundles that are too thick to be stapled in regular envelope(s), or fastened together with a rubber band.

    - Sign, date, and annotate the reason for destruction on the front(s) of the envelope(s), or top sheet, as applicable.

    - Deliver all claims-related materials, along with the claims folder(s), if

needed, for a second signature to supervisor.

- Place the two-signature claims-related documents into red envelopes or boxes after return by the supervisor.

2. The VR&E Officer or Assistant VR&E Officer will perform the following actions:

   - Review claims-related documents submitted by the employees to determine if destruction is appropriate.

   - Indicate approval by signing and dating the claims-related document(s) and returning the document(s) to the employee.

   - Review any claims-related documents that were inappropriately submitted for shredding by employee.

   - Sign and date the claims documents authorizing approval, or instruct that the documents be returned to the claims file.

   - Notify the employee when a violation has occurred.

f. Policy on the Handling and Storage of VR&E Documents and Claims when Working from Home

1. Employees engaged in work-at-home activities that involve the handling and storage of paper documents may only perform work involving the use of a CER file. Under no circumstances will loose material, not associated with a CER file, be taken to the case manager's home. CER folders may not be kept at the case manager's home for more than seven days. CER folders will be stored only in an approved lockable transporting container or in a locked file cabinet in the home.

2. Except in conjunction with approved off-site visits, VR&E employees may not take counseling folders and other sensitive information to their homes. Folders must not be left in unattended vehicles. VR&E Officers are responsible for ensuring that staff members understand and comply with this policy. He/she is responsible for purchasing any materials, such as locking briefcases, necessary to carry out this policy.

3. VR&E employees may take CER folders to a remote work location if the information is transported in a locked briefcase and if other relevant VA policy and regulations are followed during transport and at the remote location.

4. A signed copy of the rules for taking folders or information off-site, found in Appendix V, must be on file with the employee's supervisor before any information is taken off-site. The employee must complete and submit the sign-out log, Appendix AD, to his/her supervisor each time information is taken off-site and returned.

g. Policy on the Handling and Storage of VR&E Documents and Claims When Conducting Off-site and Outreach Activities

1. Employees engaged in off-site visits, outreach events, stand-downs, or other locations where VR&E applications and/or related evidence are received, must take the following actions:

   (a) Employees engaged in off-site activities that involve counseling or case management of Veterans may only perform work involving the use of a CER file. Under no circumstances will loose material not associated with a CER folder, other than blank forms utilized to gather information or complete referrals, be taken to remote locations. CER folders must be stored only in approved lockable transporting containers.

   (b) Only one file may be out on the work surface at one time.

2. Employees engaged in outreach activities for the purpose of taking claims for VR&E benefits, or who take claims during routine case management activities, including applications and evidentiary information, will take the following actions:

   (a) Provide the Servicemember or Veteran for whom evidence or a claim is taken with a dated receipt identifying the evidence received and the name of the employee who received it.

   (b) Prepare a document receipt register on which the employee will annotate the name and claim number of the Servicemember or Veteran from whom documents were received. This register must include the date, the general type of evidence received, such as applications, medical evidence, financial evidence, dependency documents, and the name of the employee who received the documents. These registers may be paper or electronic.

   (c) Secured the information and documents in an approved lockable container for transporting. All information must be hand delivered or mailed to the VR&E Office, together with a copy of the register, within 72 hours.

When applications or evidence is returned to the VR&E office, the employee will provide the documents and the register to their supervisor. A copy of the register will be maintained for six years as defined by the general statute of limitations for civil actions against the United States.

3. When VR&E staff members are meeting individually with Veterans, only the Veteran's CER file may be visible on the work surface and privacy screens will be utilized on computer screens to safeguard electronic information. At no time will a Veteran be left unattended in the temporary space, nor will CER folders or computer equipment be left in an unlocked or unsecured temporary workspace. All Veterans must be escorted to and from designated waiting areas.

4. A signed copy of the rules for taking folders or information off-site, Appendix V, must be on file with the employee's supervisor before any information may be taken off-site. The employee must complete and submit the sign-out log, Appendix AD, to the employee's supervisor each time information is taken off-site and returned.

h. Handling Veterans' Personal Information Including Mock-up Folders Provided to VR&E Contractors

1. All case managers must follow the procedures outlined below regarding the creation, retention, handling, and destroying of documents and mock-up folders provided to contractors:

   (a) CER folders will not be released to contractors. Only copies of data and documents necessary for the contractor to conduct the services requested will be placed in the mock-up folders and forwarded to contractors. Types of documents provided to the contractor will vary from case to case depending on the type of services requested and background information required to provide the services.

   (b) To ensure that the contractor does not misuse PII, any document containing personally identifying information may be released as long as safeguards are in place to protect the information and it is outlined in the contract. Refer to VA Handbook 6500.6.

   (c) Case managers must follow the guidance relating to the protection of privacy and release of information as cited in M28R.III.C.2.

   (d) Documents containing personal identifying information must be sent according to VBA's prescribed shipping method.

2. Contractors must follow the procedures outlined below regarding Veterans' files and documents:

   (a) All documents returned by contractors to the VR&E office must be sent via mail delivery service with traceable means.

   (b) As cited in the Federal Acquisition Regulations (FAR), Subpart 4.7, Contractor Records Retention, all contractors are responsible for retaining records, materials, and other evidence relating to cases and services provided to Veterans under VR&E contracts until three years after final payment has been rendered.

   (c) Contractors are required to follow the guidance relating to the privacy and security safeguards of Veterans' information as cited in FAR 52.239-1, Privacy or Security Safeguards; 52.224-1, Privacy Act Notification; and 52.224-2, Privacy Act.

   (d) Upon expiration of the retention date, contractors should provide the VR&E office certification of the destruction of such records. Certification from the contractor should include:

   - Veteran's name
   - Last four digits of Veteran's social security number
   - Type of document(s) and date(s)
   - Date of destruction
   - Means of destruction (preferably shredded)
   - Name and position of individual who destroyed document(s)

5.05 Restrictions on Use of Electronic Mail (Email) and Facsimile (Fax) Machine

VR&E staff must adhere to safeguarding privacy and confidentiality of the Veterans' information. VR&E staff must ensure that all email communications containing Veterans' PII are sent with encryptions.

VR&E staff may communicate with Veterans, VR&E contractors, and school officials through their personal or office emails. However, email communications must not contain any Veteran's PII.

VR&E contractors must not send any information with Veterans' PII via email to VA staff without appropriate encryption, as outlined in the VetSuccess Contract. The contract stipulates, "The Contractor will store, transport or transmit VA sensitive information in an encrypted form, using a VA-approved encryption application that meets the requirements of NIST's FIPS 140-2 standard, Level 2." Documentation that cannot be sent with VA-approved encryption must be sent via postal mail service with traceable means.

VA staff may send and receive documents with Veterans' PII to Veterans, VR&E contractors, and school officials using a secure fax machine. VR&E staff must inform the recipients to pick up the documentation from the fax machine as soon as transmission is completed. The confirmation of the fax transmission must be sent via email indicating the number of pages faxed and identifying information to acknowledge receipt of transmitted document.

5.06 Social Media

VR&E staff should not use their personal social media sites to communicate with Veterans, Servicemembers, and/or families regarding any VA-related discussions involving confidential or restricted information. See M28R.III.B.1 for complete procedural guidance on the use of social media.