**Table of Contents**

**Chapter 2 - Protection of Insurance Records**

|  |  |
| --- | --- |
| **Subsection** | **Name** |
| 2.01 | Confidential Nature of Information in Insurance Records |
| 2.02 | Sensitive Files |
| 2.03 | Protection of Original Physical Records Against Defacement |
| 2.04  | Archiving and/or Destruction of Paper Records |
| 2.05 | Insurance Records Maintained in Insurance Program Management Division |
| 2.06 | Freedom Of Information Act (FOIA) And Privacy Act (PA) Guidance |

**2.01   CONFIDENTIAL NATURE OF INFORMATION IN INSURANCE RECORDS**

Preservation of record content is a prime consideration of personnel handling Veterans' Insurance records. The information contained in the retired insurance folders or in electronic records is privileged and confidential. VA personnel will not review or discuss information from either source except to the extent required for the performance of their official duties.

**2.02   SENSITIVE FILES**

a.     Sensitive File Insurance Records will be established and maintained, electronically, in the Insurance system. Sensitive files will be established at different levels, depending on the level of confidentiality required. Sensitive files will include all insurance records of a restricted nature. The Assistant Director, Operations, Division Chiefs, or certain other authorized personnel will be responsible for the safeguarding and release, upon proper request, of all sensitive material.

b.    The sensitive files include:

1.    Insured records with sensitivity levels of 6-9 as noted in the table below:

|  |  |  |
| --- | --- | --- |
|  Level of Sensitivity | Insurance Records Including Employees, Veterans or Their Beneficiaries |  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  | 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 | Facility Directors and assistants; Area Directors; VSC Managers and Assistants; all other Division Chiefs |
| 7 | VBA employees; private attorney fee cases | ISOs 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. | 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 | Local Use Determination | Records of employees, relatives of employees, legislatures, and public figures that have VA life insurance.  Based on grade/position and job duties. |
| 4 | Local Use Determination | Records of employees, relatives of employees, legislatures, and public figures that have VA life insurance.  Based on grade/position and job duties. |
| 3 | Local Use Determination | Records of employees, relatives of employees, legislatures, and public figures that have VA life insurance.  Based on grade/position and job duties. |
| 2 | Local Use Determination | Based on grade/position and job duties. |
| 1 | Local Use Determination | Based on grade/position and job duties. |

2.    With reports from the FBI (Federal Bureau of Investigation)

3.    Listed as being missing in action (MIA)

4.    Who have an active tax levy from the IRS or VA benefits

c.     All other records which the Director determines should be marked sensitive because of the nature of their content or public interest in the veterans concerned, will be maintained in the Office of the Director.

d.      Employee-Veterans are permitted to see their own records upon request; however, access must be supervised. Requests for information from employees' records will be routed through normal channels.

e.      Representatives of other federal agencies, having been authorized to examine sensitive files through proper identification and certification by a designated VA official, will be required to sign a VA Form 119, Report of Contact, showing the date and time of inspection, identification of the record examined, the purpose of the examination and identification of the representative.

f.      The table above reflects the revised sensitivity levels for the BDN as well as Common Security Services (VETSNET).  All sensitive level access requests must be submitted in CSEM, or using the VA-8824e for offices not currently using CSEM, for concurrence and approval by the Station Director, Acting Station Director or Assistant Director.  Level 8 and 9 may be given to employees with designated positions as listed in the attachment.  Level 7 restrictions are limited to a maximum of 10 percent of non-supervisory staff allowed access.  Level 6 access is limited to an additional 25 percent of non-supervisory staff, with the stipulation that such access be given only to journey level employees.  Therefore, a total of 35 percent of employees are entitled to Level 6 access and above, to include VR&E employees.  Designation of journey level status and business need is a management decision.  All other employees should remain at level 0.

**2.03   PROTECTION OF ORIGINAL PHYSICAL RECORDS AGAINST DEFACEMENT**

Physical records, prior to being scanned for storage in the Insurance system by Clerical Support, will not be stamped or marked in any manner other than those prescribed in VA procedures, nor will numbers or marks of any kind be placed on records or documents in a manner that will obliterate or deface any part of the contents. Extreme care will be exercised in using stamp impressions, staplers and perforators, and in making comments, notations or underscoring. Under no circumstances will any VA record or document in temporary custody of VA, which is to be returned to the sender, be *crumpled* or *marred.*

**2.04   ARCHIVING AND/OR DESTRUCTION OF PAPER RECORDS**

After physical records have been properly scanned for storage in the Insurance system, they will be handled in accordance with the VBA Records Control Schedule (RCS).  The RCS is a document that identifies types of records, and provides retention and disposition authority and timeframes. If a record can be destroyed, per the RCS, it must be in accordance with the procedures outlined in VBA Directive 6300. Insurance specific guidelines can be found in VBA Directive 6300 Appendix B.

**2.05   INSURANCE RECORDS MAINTAINED IN INSURANCE PROGRAM MANAGEMENT DIVISION**

There are no physical records stored or maintained in the Insurance Program Management Division (IPMD).   Electronic records are stored on a shared drive, accessible only to authorized personnel.

**2.06 FREEDOM OF INFORMATION ACT (FOIA) AND PRIVACY ACT (PA) GUIDANCE**

a.    FOIA and PA are two laws that guide whether VA can release information.

1.    Freedom of Information Act – provides individuals rights to access Federal agency records, except to the extent those records are protected from release by a FOIA exemption or special law enforcement exclusion.

2.    Privacy Act – balances the government’s need to maintain information about individuals with the rights of individuals to be protected against unwarranted invasions of privacy.

3.    Insurance policy for FOIA and PA is based on VA Directive 6300, VBA Handbook 6502, VA Handbook 6300.3.  Employees should review these policies as well as any additional Insurance-specific policy to determine the appropriate process for handling requests for release of records before releasing the records.  If needed, employees should seek guidance from their supervisory chain and the Insurance FOIA and/or Privacy Officers.