§ 74.29 When will VA dispose of records?

The records, including those pertaining to businesses not determined to be eligible for the program, will be kept intact and in good condition for seven years following a program examination or the date of the last Notice of Verified Status Approval letter. Longer retention will not be required unless a written request is received from the Government Accountability Office not later than 30 days prior to the end of the retention period.

(Authority: 38 U.S.C. 8127(f))

PART 75—INFORMATION SECURITY MATTERS

Subpart A [Reserved]

Subpart B—Data Breaches

Sec. 75.111 Purpose and scope.
75.112 Definitions and terms.
75.113 Data breach.
75.114 Accelerated response.
75.115 Risk analysis.
75.116 Secretary determination.
75.117 Notification.
75.118 Other credit protection services.
75.119 Finality of Secretary determination.


Source: 72 FR 34399, June 22, 2007, unless otherwise noted.

Subpart A [Reserved]

Subpart B—Data Breaches

§ 75.111 Purpose and scope.

This subpart implements provisions of 38 U.S.C. 5724 and 5727, which are set forth in Title IX of the Veterans Benefits, Health Care, and Information Technology Act of 2006. It only concerns actions to address a data breach regarding sensitive personal information that is processed or maintained by VA. This subpart does not supersede the requirements imposed by other laws, such as the Privacy Act of 1974, the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996, the Fair Credit Reporting Act, and implementing regulations of such Acts.

(Authority: 38 U.S.C. 501, 5724, 5727)

§ 75.112 Definitions and terms.

For purposes of this subpart:
Confidentiality means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information.

Data breach means the loss or theft of, or other unauthorized access to, data containing sensitive personal information, in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data.

Data breach analysis means the process used to determine if a data breach has resulted in the misuse of sensitive personal information.

Fraud resolution services means services to assist an individual in the process of recovering and rehabilitating the credit of the individual after the individual experiences identity theft.

Identity theft has the meaning given such term under section 603 of the Fair Credit Reporting Act (15 U.S.C. 1681a).

Identity theft insurance means any insurance policy that pays benefits for costs, including travel costs, notary fees, and postage costs, lost wages, and legal fees and expenses associated with efforts to correct and ameliorate the effects and results of identity theft of the insured individual.

Individual means a single human being who is a citizen of the United States, an alien admitted to permanent residence in the United States, a present or former member of the Armed Forces, or any dependent of a present or former member of the Armed Forces.

Information system means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information, whether automated or manual.

Integrity means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
§ 75.113 Logical data access means the ability of a person to translate the data for misuse. This can lead to inappropriate access to lost, stolen or improperly obtained data.

Person means an individual; partnership; corporation; Federal, State, or local government agency; or any other legal entity.

Processed or maintained by VA means created, stored, transmitted, or manipulated by VA personnel or by a person acting on behalf of VA, including a contractor or other organization or any level of subcontractor or other suborganization.

Secretary means the Secretary of Veterans Affairs or designee.

Sensitive personal information, with respect to an individual, means any information about the individual maintained by an agency, including the following:

(1) Education, financial transactions, medical history, and criminal or employment history.

(2) Information that can be used to distinguish or trace the individual’s identity, including name, Social Security number, date and place of birth, mother’s maiden name, or biometric records.

Unauthorized access incidental to the scope of employment means access, in accordance with VA data security and confidentiality policies and practices, that is a by-product or result of a permitted use of the data, that is inadvertent and cannot reasonably be prevented, and that is limited in nature.

VA means the Department of Veterans Affairs.

(Authority: 38 U.S.C. 501, 5724, 5727)

§ 75.114 Accelerated response.

(a) The Secretary, in the exercise of his or her discretion, may provide notice to records subjects of a data breach and/or offer them other credit...
protection services prior to the completion of a risk analysis if:
(1) The Secretary determines, based on the information available to the agency when it learns of the data breach, that there is an immediate, substantial risk of identity theft of the individuals whose data was the subject of the data breach, and providing timely notice may enable the record subjects to promptly take steps to protect themselves, and/or the offer of other credit protection services will assist in timely mitigation of possible harm to individuals from the data breach; or
(2) Private entities would be required to provide notice under Federal law if they experienced a data breach involving the same or similar information.
(3) In situations described in paragraphs (a)(1) or (a)(2) of this section, the Secretary may provide notice of the breach prior to completion of a risk analysis, and subsequently advise individuals whether the agency will offer additional credit protection services upon completion, and consideration of the results, of the risk analysis, if the Secretary directs that one be completed.
(b) In determining whether to promptly notify individuals and/or offer them other credit protection services under paragraph (a)(1) of this section, the Secretary shall make the decision based upon the totality of the circumstances and information available to the Secretary at the time of the decision, including whether providing notice and offering other credit protection services would be likely to assist record subjects in preventing, or mitigating the results of, identity theft based on the compromised VA sensitive personal information. The Secretary’s exercise of this discretion will be based on good cause, including consideration of the following factors:
(1) The nature and content of the lost, stolen or improperly accessed data, e.g., the data elements involved, such as name, social security number, date of birth;
(2) The ability of an unauthorized party to use the lost, stolen or improperly accessed data, either by itself or with data or applications generally available, to commit identity theft or otherwise misuse the data to the disadvantage of the record subjects, if able to access and use the data;
(3) Ease of logical data access to the lost, stolen or improperly accessed data in light of the degree of protection for the data, e.g., unencrypted, plain text;
(4) Ease of physical access to the lost, stolen or improperly accessed data, e.g., the degree to which the data is readily available to unauthorized access, such as being in a dumpster readily accessible by members of the general public;
(5) The format of the lost, stolen or improperly accessed data, e.g., in a standard electronic format, such as ASCII, or in paper;
(6) Evidence indicating that the lost, stolen or improperly accessed data may have been the target of unlawful acquisition; and
(7) Evidence that the same or similar data had been acquired from other sources improperly and used for identity theft.
(c) VA will provide notice and/or other credit protection services under this section as provided in §§ 75.117 and 75.118.

(Authority: 38 U.S.C. 501, 5724, 5727)

§ 75.115 Risk analysis.

If a data breach involving sensitive personal information that is processed or maintained by VA occurs and the Secretary has not determined under § 75.114 that an accelerated response is appropriate, the Secretary shall ensure that, as soon as possible after the data breach, a non-VA entity with relevant expertise in data breach assessment and risk analysis or VA’s Office of Inspector General conducts an independent risk analysis of the data breach. The preparation of the risk analysis may include data mining if necessary for the development of relevant information. The risk analysis shall include a finding with supporting rationale concerning whether the circumstances create a reasonable risk that sensitive personal information potentially may be misused. If the risk analysis concludes that the data breach presents a reasonable risk for the potential misuse of sensitive personal information, the risk analysis

1115
must also contain operational recommendations for responding to the data breach. Each risk analysis, regardless of findings and operational recommendations, shall also address all relevant information concerning the data breach, including the following:

(a) Nature of the event (loss, theft, unauthorized access).

(b) Description of the event, including:

(1) Date of occurrence;
(2) Data elements involved, including any personally identifiable information, such as full name, social security number, date of birth, home address, account number, disability code;
(3) Number of individuals affected or potentially affected;
(4) Individuals or groups affected or potentially affected;
(5) Ease of logical data access to the lost, stolen or improperly accessed data in light of the degree of protection for the data, e.g., unencrypted, plain text;
(6) Time the data has been out of VA control;
(7) The likelihood that the sensitive personal information will or has been made accessible to and usable by unauthorized persons;

(c) Assessment of the potential harm to the affected individuals.

(d) Data breach analysis, as appropriate.

(Authority: 38 U.S.C. 501, 5724, 5727)

§ 75.117 Notification.

(a) With respect to individuals found under this subpart by the Secretary to be subject to a reasonable risk for the potential misuse of any sensitive personal information, the Secretary will promptly provide written notification by first-class mail to the individual (or the next of kin if the individual is deceased) at the last known address of the individual. The notification may be sent in one or more mailings as information is available and will include the following:

(1) A brief description of what happened, including the date[s] of the data breach and of its discovery if known;
(2) To the extent possible, a description of the types of personal information that were involved in the data breach (e.g., full name, Social Security
number, date of birth, home address, account number, disability code); (3) A brief description of what the agency is doing to investigate the breach, to mitigate losses, and to protect against any further breach of the data; (4) Contact procedures for those wishing to ask questions or learn additional information, which will include a toll-free telephone number, an e-mail address, Web site, and/or postal address; (5) Steps individuals should take to protect themselves from the risk of identity theft, including steps to obtain fraud alerts (alerts of any key changes to such reports and on demand access to credit reports and scores), if appropriate, and instruction for obtaining other credit protection services offered under this subpart; and (6) A statement whether the information was encrypted or protected by other means, when determined such information would be beneficial and would not compromise the security of the system. (b) In those instances where there is insufficient, or out-of-date contact information that precludes direct written notification to an individual subject to a data breach, a substitute form of notice may be provided, such as a conspicuous posting on the home page of VA’s Web site and notification in major print and broadcast media, including major media in geographic areas where the affected individuals likely reside. Such a notice in media will include a toll-free phone number where an individual can learn whether or not his or her personal information is possibly included in the data breach. (c) In those cases deemed by the Secretary to require urgency because of possible imminent misuse of sensitive personal information, the Secretary, in addition to notification under paragraph (a) of this section, may provide information to individuals by telephone or other means, as appropriate. (d) Notwithstanding other provisions in this section, notifications may be delayed upon lawful requests, from other Federal agencies, for the delay of notifications in order to protect data or computer resources from further compromise or to prevent interference with the conduct of an investigation or efforts to recover the data. A lawful request is one made in writing by the entity or VA component responsible for the investigation or data recovery efforts that may be adversely affected by providing notification. Any lawful request for delay in notification must state an estimated date after which the requesting entity believes that notification will not adversely affect the conduct of the investigation or efforts to recover the data. However, any delay should not exacerbate risk or harm to any affected individual(s). Decisions to delay notification should be made by the Secretary. (Authority: 38 U.S.C. 501, 5724, 5727) § 75.118 Other credit protection services. (a) With respect to individuals found under this subpart by the Secretary to be subject to a reasonable risk for the potential misuse of any sensitive personal information under this subpart, the Secretary may offer one or more of the following as warranted based on considerations specified in paragraph (b) of this section: (1) One year of credit monitoring services consisting of automatic daily monitoring of at least 3 relevant credit bureau reports; (2) Data breach analysis; (3) Fraud resolution services, including writing dispute letters, initiating fraud alerts and credit freezes, to assist affected individuals to bring matters to resolution; and/or (4) One year of identity theft insurance with $20,000.00 coverage at $0 deductible. (b) Consistent with the requirements of the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.) as interpreted and applied by the Federal Trade Commission, the notice to the individual offering other credit protection services will explain how the individual may obtain the services, including the information required to be submitted by the individual to obtain the services, and the time period within which the individual must act to take advantage of the credit protection services offered. (c) In determining whether any or all of the credit protection services specified in paragraph (a) of this section will be offered to individuals subject to a
1118

§ 75.119 Finality of Secretary determination.

A determination made by the Secretary under this subpart will be a final agency decision.

PART 76—MONTHLY ASSISTANCE ALLOWANCE FOR VETERANS IN CONNECTION WITH THE UNITED STATES PARALYMPICS

Sec.
76.1 Definitions.
76.2 Assistance allowance.
76.3 Application and certification.
76.4 Amount of allowance.

AUTHORITY: 38 U.S.C. 501, 322(d), and as stated in specific sections.

SOURCE: 76 FR 14283, Mar. 16, 2011, unless otherwise noted.

§ 76.1 Definitions.

For purposes of part 76, the following definitions apply:

Disability means a service-connected or nonservice-connected disability which meets the criteria prescribed by the International Paralympic Committee (IPC) Classification Code and International Standards, November 2007 edition, available at http://www.paralympic.org/export/sites/default/IPC/IPC_Handbook/Section_2/2008_2_Classification_Code6.pdf, and qualifies the veteran for participation in a sport sanctioned by the United States Paralympics. The IPC standards are incorporated by reference into this section with the approval of the Director of the Federal Register under 5 U.S.C. 552(a) and 1 CFR part 51. To enforce any edition other than that specified in this section, VA must publish notice of change in the Federal Register and the material must be available to the public.

(1) You may obtain a copy from the International Paralympic Committee at International Paralympic Committee, Adenauerallee 212-214, 53113 Bonn, Germany.

(2) All approved material is available for inspection at the Department of Veterans Affairs, Office of Regulation Policy and Management (02REG), Room 1063B, 810 Vermont Avenue, NW., Washington, DC 20420, or at the National Archives and Records Administration (NARA). For information on the availability of approved materials at NARA, call (202) 741-6030, or go to: http://www.archives.gov/federal_register/code_of_federal_regulations/ibr_locations.html. The IPC standards are also available here: http://www.va.gov/ABOUT VA/docs/ParalympicClassificationCode.pdf.

(Authority: 38 U.S.C. 322(d))

§ 76.2 Assistance allowance.

(a) VA will pay an allowance to a veteran with a disability who is:

(1) Invited by the United States Olympic Training Center at Chula Vista, California; the United States Olympic Training Center at Colorado Springs, Colorado; the United States Olympic Training Center at Lake Placid, New York; the Lakeshore Foundation in Birmingham, Alabama; and the University of Central Oklahoma in Edmond, Oklahoma.

(Authority: 38 U.S.C. 322(d))

§ 76.3 Application and certification.

(a) VA will pay an allowance to a veteran with a disability who is:

(1) Invited by the United States Paralympics (USP) to compete for a slot on, or selected for, the USP Team for any month or part of any month in which the veteran is training or competing in any event sponsored by the USP or the IPC; or

(2) Residing at a USP training center in connection with any paralympic training or competition for the period certified under §76.3.

(Authority: 38 U.S.C. 322(d))