

Department of Veterans Affairs

§ 75.112

numbers for veterans, service-disabled veterans and surviving spouses who represent themselves as having ownership and control interests in a specific business seeking to obtain verified status.

§ 74.26 What types of business information will VA collect?

VA will examine a variety of business records. See § 74.12, “What is a verification examination and what will CVE examine?”

§ 74.27 How will VA store information?

VA intends to store records provided to complete the VetBiz Vendor Information Pages registration fully electronically on the Department’s secure servers. CVE personnel will compare information provided concerning owners who have veteran status, service-disabled veteran status or surviving spouse status against electronic records maintained by the Department’s Veterans Benefits Administration. Records collected during examination visits will be scanned onto portable media and fully secured in the Center for Veterans Enterprise, located in Washington, DC.

§ 74.28 Who may examine records?

Personnel from the Department of Veterans Affairs, Center for Veterans Enterprise and its agents, including personnel from the Small Business Administration, may examine records to ascertain the ownership and control of the applicant or participant.

§ 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.

AUTHORITY: 38 U.S.C. 501, 5724, 5727, 7906.

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, other than an unauthorized access incidental to the scope of employment, data containing sensitive personal information, in electronic or printed

§ 75.113

38 CFR Ch. I (7–1–14 Edition)

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.

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)

§ 75.113 Data breach.

Consistent with the definition of data breach in § 75.112 of this subpart, a data breach occurs under this subpart if there is a loss or theft of, or other unauthorized access to, other than an unauthorized access incidental to the scope of employment, data containing sensitive personal information, in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data. The term “unauthorized access” used in the definition of “data breach” includes access to an electronic information system and includes, but is not limited to, viewing, obtaining, or using data containing sensitive personal information in any form or in any VA information system. The phrase “unauthorized access incidental to the scope of employment” includes instances when employees of contractors and other entities need access to VA sensitive information in order to perform a contract or agreement with VA but incidentally obtain access to other VA sensitive information. Accordingly, an unauthorized access, other than an unauthorized access incidental to the