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 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 scope of employment, 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, constitutes a data breach. In addition to these circumstances, VA also interprets data breach to include circumstances in which a user misuses sensitive personal information to which he or she has authorized access. The following circumstances do not constitute a data breach and, consequently, are not subject to the provisions of this subpart:

(a) An unauthorized access to data containing sensitive personal information that was determined by the Secretary to be incidental to the scope of employment, such as an inadvertent unauthorized viewing of sensitive personal information by a VA employee or a person acting on behalf of VA.

(b) A loss, theft, or other unauthorized access to data containing sensitive personal information that the Secretary determined to have no possibility of compromising the confidentiality or integrity of the data, such as the inability of compromising the confidentiality or integrity of the data because of encryption or the inadvertent disclosure to another entity that is required to provide the same or a similar level of protection for the data under statutory or regulatory authority.

(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: