

## § 75.115

(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 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;

## 38 CFR Ch. I (7-1-08 Edition)

(6) Time the data has been out of VA control;

(7) The likelihood that the sensitive personal information will or has been compromised (made accessible to and usable by unauthorized persons); and

(8) Known misuses of data containing sensitive personal information, if any.

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

(d) Data breach analysis, as appropriate.

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

### § 75.116 Secretary determination.

(a) Upon receipt of a risk analysis prepared under this subpart, the Secretary will consider the findings and other information contained in the risk analysis to determine whether the data breach caused a reasonable risk for the potential misuse of sensitive personal information. If the Secretary finds that such a reasonable risk does not exist, the Secretary will take no further action under this subpart. However, if the Secretary finds that such a reasonable risk exists, the Secretary will take responsive action as specified in this subpart based on the potential harms to individuals subject to a data breach.

(b) In determining whether the data breach resulted in a reasonable risk for the potential misuse of the compromised sensitive personal information, the Secretary shall consider all factors that the Secretary, in his or her discretion, considers relevant to the decision, including:

(1) The likelihood that the sensitive personal information will be or has been made accessible to and usable by unauthorized persons;

(2) Known misuses, if any, of the same or similar sensitive personal information;

(3) Any assessment of the potential harm to the affected individuals provided in the risk analysis;

(4) Whether the credit protection services that VA may offer under 38 U.S.C. 5724 may assist record subjects in avoiding or mitigating the results of identity theft based on the VA sensitive personal information that had been compromised;

(5) Whether private entities are required under Federal law to offer credit protection services to individuals if the