§ 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. 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:

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

(2) 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 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)