AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

(b) The hardware, modem and software utilized to obtain access, as well as their location, must be approved in advance by VBA.

(c) Each individual and organization approved for access must sign and return a notice provided by the Regional Office Director (or the Regional Office Director's designee) of the Regional Office of jurisdiction for the claim. The notice will specify the applicable operational and security requirements for access and an acknowledgment that the breach of any of these requirements is grounds for disqualification from access.

[59 FR 47084, Sept. 14, 1994. Redesignated at 73 FR 29870, May 22, 2008]

§ 1.602 Utilization of access.

(a) Once an individual or organization has been issued the necessary passwords to obtain read-only access to the automated claims records of individuals represented, access will be exercised in accordance with the following requirements:

(1) The individual or organization will obtain access only from equipment and software approved in advance by the Regional Office from the location where the individual or organization primarily conducts its representation activities which also has been approved in advance;

(2) The individual will use only his or her assigned password to obtain access;

(3) The individual will not reveal his or her password to anyone else, or allow anyone else to use his or her password;

(4) The individual will access only the VBA automated claims records of VA claimants who are represented by the person obtaining access or by the organization employing the person obtaining access;

(5) The individual will access a claimant's automated claims record solely for the purpose of representing that claimant in a claim for benefits administered by VA;

(6) Upon receipt of the password, the individual will destroy the hard copy; no written or printed record containing the password will be retained; and

(7) The individual and organization will comply with all security requirements VBA deems necessary to ensure the integrity and confidentiality of the data and VBA's automated computer systems.

(b) An organization granted access shall ensure that all employees provided access in accordance with these regulations will receive regular, adequate training on proper security, including the items listed in §1.603(a). Where an individual such as an attorney or registered agent is granted access, he or she will regularly review the security requirements for the system as set forth in these regulations and in any additional materials provided by VBA.

(c) VBA may, at any time without notice:

(1) Inspect the computer hardware and software utilized to obtain access and their location;

(2) Review the security practices and training of any individual or organization granted access under these regulations; and

(3) Monitor an individual's or organization's access activities. By applying for, and exercising, the access privileges under §§1.600 through 1.603, the applicant expressly consents to VBA monitoring the access activities of the applicant at any time.

[59 FR 47084, Sept. 14, 1994. Redesignated and amended at 73 FR 29870, 29879, May 22, 2008]

§ 1.603 Disqualification.

(a) The Regional Office Director or the Regional Office Director's designee may revoke an individual's or an organization's access privileges to a particular claimant's records because the individual or organization no longer represents the claimant, and, therefore, the beneficiary's consent is no longer in effect. The individual or organization is no longer entitled to access as a matter of law under the Privacy Act, 5 U.S.C. 552a, and 38 U.S.C. 5701 and 7332. Under these circumstances, the individual or organization is not entitled to any hearing or to present any evidence in opposition to the revocation.

(b) The Regional Office Director or the Regional Office Director's designee may revoke an individual's or an organization's access privileges either to an individual claimant's records or to all