14. Disclosure of any information within this system may be made when it is suspected or confirmed that the security or confidentiality of information in the system of records has been compromised and VA has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interest, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by VA or another agency or entity) that rely upon the compromised information; and the disclosure is made to such agencies, entities, and persons who are reasonably necessary to assist in connection with VA's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:

Records are maintained on paper and on electronic storage media, including magnetic tape, disk, encrypted flash memory, and laser optical media.

RETRIEVABILITY:

Records are retrieved by name, Social Security Number, or other assigned identifiers of the individuals on whom they are maintained.

SAFEGUARDS:

1. Access to and use of national patient databases are limited to those persons whose official duties require such access, and VA has established security procedures to ensure that access is appropriately limited. Information security officers and system data stewards review and authorize data access requests. VA regulates data access with security software that authenticates users and requires individually unique codes and passwords. VA provides information security training to all staff and instructs staff on the responsibility each person has for safeguarding data confidentiality.

2. VA maintains Business Associate Agreements (BAA) and Non-Disclosure Agreements with contracted resources in order to maintain confidentiality of the information.

3. Physical access to computer rooms housing national patient databases is restricted to authorized staff and protected by a variety of security devices. Unauthorized employees, contractors, and other staff are not allowed in computer rooms. The Federal Protective Service or other security personnel provide physical security for the buildings housing computer rooms and data centers.

4. All materials containing real or scrambled Social Security Numbers are kept only on secure, encrypted VHA servers, personal computers, laptops, or media. All e-mail transmissions of such files use Public Key Infrastructure (PKI) encryption. If a recipient does not have PKI, items are mailed or sent to a secure fax. Paper records containing Social Security Numbers are secured in locked cabinets or offices within the OMI area. Access to OMI requires passing a security officer, an elevator card reader for floor access and a separate VHA card reader for access to the office area. All materials, both paper and electronic, that are no longer required are shredded/obliterated in accordance with VHA guidelines. Materials required for case documentation and follow up are archived in our secure document management server (electronic) and in locked storage (paper).

5. In most cases, copies of back-up computer files are maintained at off-site locations.

RETENTION AND DISPOSAL:

The records are disposed of in accordance with Section XXXV—Office of the Medical Inspector (10MI) of the Veterans Health Administration Records Control Schedule 10–1 of March 31, 2008, which stipulates that records from investigations not involving site visits will be destroyed 10 years after closure; records from investigations involving site visits will be destroyed 20 years after closure.

SYSTEM MANAGER(S) AND ADDRESS:

Official responsible for policies and procedures; Chief Information Officer (19), Department of Veterans Affairs, 810 Vermont Avenue, NW., Washington, DC 20420. Official maintaining this system of records: Donald L. Martin, Correspondence Analyst, OMI (10MI), 810 Vermont Avenue, NW., Washington, DC 20420.

NOTIFICATION PROCEDURE:

Individuals who wish to determine whether this system of records contains information about them should contact Donald L. Martin, Correspondence Analyst, OMI (10MI), 810 Vermont Avenue, NW., Washington, DC 20420. Inquiries should include the person's full name, Social Security number, location and dates of employment or location and dates of treatment, and return address.

RECORD ACCESS PROCEDURE:

Individuals seeking information regarding access to and contesting of records in this system may write or call Donald L. Martin, Correspondence Analyst, OMI (10MI), 810 Vermont Avenue, NW., Washington, DC 20420, 202–461–4079.

CONTESTING RECORD PROCEDURES:

(*See* Record Access Procedures above.)

RECORD SOURCE CATEGORIES:

Information in this system of records is provided by Veterans, VA employees, VA computer systems, Veterans Health Information Systems and Technology Architecture (VistA), VA medical centers, VA Health Eligibility Center, VA program offices, VISNs, VA Austin Automation Center, the Food and Drug Administration, the Department of Defense, Survey of Healthcare Experiences of Patients, External Peer Review Program, and the following Systems Of Records: "Patient Medical Records—VA" (24VA19), "National Prosthetics Patient Database—VA" (33VA113), "Healthcare Eligibility Records—VA" (89VA16), VA Veterans Benefits Administration automated record systems (including the Veterans and Beneficiaries Identification and Records Location Subsystem—VA (38VA23), and subsequent iterations of those systems of records.

[FR Doc. 2010–11373 Filed 5–11–10; 8:45 am]

BILLING CODE 8320–01–P

DEPARTMENT OF VETERANS AFFAIRS

Privacy Act of 1974; System of Records

AGENCY: Department of Veterans Affairs (VA).

ACTION: Notice of amendment to System of Records.

SUMMARY: As required by the Privacy Act of 1974, 5 U.S.C. 552a(e), notice is hereby given that the Department of Veterans Affairs (VA) is amending the system of records currently entitled "Veterans Canteen Service (VCS) Payroll Deduction Program (PDP)-VA" (117VA103) as set forth in the **Federal Register** 71 FR 6133. VA is amending the system of records by revising the Routine Uses of Records Maintained in the System, Including Categories of Users and the Purposes of Such Uses. VA is republishing the system notice in its entirety.

DATES: Comments on the amendment of this system of records must be received no later than June 11, 2010. If no public comment is received, the amended system will become effective June 11, 2010.

ADDRESSES: Written comments may be submitted through *http://www.Regulations.gov;* by mail or hand-delivery to Director, Regulations Management (02REG), Department of Veterans Affairs, 810 Vermont Avenue, NW., Room 1068, Washington, DC 20420; or by fax to (202) 273–9026. Comments received will be available for public inspection in the Office of Regulation Policy and Management, Room 1063B, between the hours of 8 a.m. and 4:30 p.m., Monday through Friday (except holidays). Please call (202) 461–4902 (this is not a toll-free number) for an appointment. In addition, during the comment period, comments may be viewed online through the Federal Docket Management System (FDMS) at *http://www.Regulations.gov*.

FOR FURTHER INFORMATION CONTACT: Veterans Health Administration (VHA) Privacy Officer, Department of Veterans Affairs, 810 Vermont Avenue, NW., Washington, DC 20420; telephone (704) 245–2492.

SUPPLEMENTARY INFORMATION:

A new Routine Use eleven (11) allows VA to disclose information from this system of records to the Department of Justice (DoJ), either on VA's initiative or in response to DoJ's request for the information, after either VA or DoJ determines that such information is relevant to DoJ's representation of the United States or any of its components in legal proceedings before a court or adjudicative body, provided that, in each case, the agency also determines prior to disclosure that release of the records to the DoJ is a use of the information contained in the records that is compatible with the purpose for which VA collected the records. VA, on its own initiative, may disclose records in this system of records in legal proceedings before a court or administrative body after determining that the disclosure of the records to the court or administrative body is a use of the information contained in the records that is compatible with the purpose for which VA collected the records.

A new Routine Use twelve (12) allows VA to disclose on its own initiative any information in the system, except the names and home addresses of Veterans and their dependents, that is relevant to a suspected or reasonably imminent violation of the law whether civil, criminal, or regulatory in nature and whether arising by general or program statute or by regulation, rule, or order issued pursuant thereto, to a Federal, State, local, tribal, or foreign agency charged with the responsibility of investigating or prosecuting such violation, or charged with enforcing or implementing the statute, regulation, rule, or order. VA may also disclose on its own initiative the names and addresses of Veterans and their dependents to a Federal agency charged with the responsibility of investigating or prosecuting civil, criminal, or regulatory violations of law, or charged with enforcing or implementing the statute, regulation, or order issued pursuant thereto.

A new Routine Use thirteen (13) allows disclosure to other Federal agencies may be made to assist such agencies in preventing and detecting possible fraud or abuse by individuals in their operations and programs. This routine use permits disclosures by the Department to report a suspected incident of identity theft and provide information and/or documentation related to or in support of the reported incident.

A new Routine Use fourteen (14) allows VA to disclose any information or records to appropriate agencies, entities, and persons when (1) VA suspects or has confirmed that the integrity or confidentiality of information in the system of records has been compromised; (2) the Department has determined that as a result of the suspected or confirmed compromise, there is a risk of embarrassment or harm to the reputations of the record subjects, harm to economic or property interests, identity theft or fraud, or harm to the security, confidentiality, or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the potentially compromised information; and (3) the disclosure is to agencies, entities, or persons whom VA determines are reasonably necessary to assist or carry out the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm. This routine use permits disclosures by the Department to respond to a suspected or confirmed data breach, including the conduct of any risk analysis or provision of credit protection services as provided in 38 U.S.C. 5724, as the terms are defined in 38 U.S.C. 5727.

The Report of Intent to Amend a System on Records Notice and an advance copy of the system notice have been sent to the appropriate Congressional committees and to the Director of the Office of Management and Budget (OMB) as required by 5 U.S.C. 552a(r) (Privacy Act) and guidelines issued by OMB (65 FR 77677), December 12, 2000.

Approved: April 15, 2010.

John R. Gingrich,

Chief of Staff, Department of Veterans Affairs.

117VA103

SYSTEM NAME: "VETERAN CANTEEN SERVICE (VCS) PAYROLL DEDUCTION SYSTEM (PDS)—VA".

SYSTEM LOCATION:

Individual purchase records are maintained in the VCS office at each Department of Veterans Affairs (VA) health care facility. Addresses for VA facilities are listed in VA Appendix 1. In addition, information from these records or copies of records are maintained in a centralized electronic database at the Austin Automation Center (AAC), 1615 East Woodward Street, Austin TX, 78772.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

The individuals covered by the system encompass permanent VA employees, also known as customers, who participate in the VCS Payroll Deduction System, which permits them to pay for purchases in VCS canteens through deduction from their pay.

CATEGORIES OF RECORDS IN THE SYSTEM:

These records include the following information:

—Customer identification information such as last name, first name, middle initial, social security number;
—Customer purchases made under the program;
—Payroll payments, cash payments, refunds for returned merchandise, and refunds for overpayments;
—Customer account balances and amounts written-off as uncollectible;
—Customer pay status when customer is in a "without pay" status;
—Identification of VCS employees creating customer transactions is by manual or electronic data capture. Manual transactions can be traced by a user ID within the payroll deduction system that identifies the individual entering the manual transaction. Electronic transactions can be traced via cashier code of the cashier ringing the transaction into the cash register; and
—Customer station number and canteen of purchase.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Title 38, United States Code, Part V, Chapter 78.

PURPOSE(S):

The records and information will be used to track customer purchases, payment and balances due to VCS. Records may also be used to identify and submit to a customer for the purpose of debt collection. The records and information may be used for management and analysis reports of VCS programs.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

To the extent that records contained in the system include information protected by 45 CFR parts 160 and 164, *i.e.,* individually identifiable health information, and 38 U.S.C. 7332, *i.e.,* medical treatment information related to drug abuse, alcoholism or alcohol abuse, sickle cell anemia or infection with the human immunodeficiency virus, that information cannot be disclosed under a routine use unless there is also specific statutory authority in 38 U.S.C. 7332 and regulatory authority in 45 CFR parts 160 and 164 permitting disclosure.

1. VA may disclose information from this system of records to a private debt collection agent for the purpose of collecting unpaid balances from customers who have left VA employment without making full payment for purchases made under the program.

2. VA may disclose information from this system of records to the U.S. Treasury Offset Program (TOPS) for the purpose of collecting unpaid balances from customers who have left VA employment without making full payment for purchases made under the program. VA needs to be able to collect unpaid balances from customers who have left VA employment without making full payment to VCS for purchases made under the program.

3. Disclosure may be made to the Federal Labor Relations Authority (FLRA), including its General Counsel, when requested in connection with investigation and resolution of allegations of unfair labor practices, in connection with the resolution of exceptions to arbitrator awards when a question of material fact is raised, and in connection with matters before the Federal Service Impasses Panel. The release of information to FLRA from this Privacy Act system of records is necessary to comply with the statutory mandate under which FLRA operates.

4. Disclosure may be made to officials of labor organizations recognized under 5 U.S.C. chapter 71 when relevant and necessary to their duties of exclusive representation concerning personnel policies, practices, and matters affecting working conditions.

5. Disclosure may be made to officials of the Merit Systems Protection Board, including the Office of the Special Counsel, when requested in connection with appeals, special studies of the civil service and other merit systems, review of rules and regulations, investigation of alleged or possible prohibited personnel practices, and such other functions promulgated in 5 U.S.C. 1205 and 1206, or as may be authorized by law.

6. Disclosure may be made to the Equal Employment Opportunity Commission when requested in connection with investigations of alleged or possible discrimination practices, examination of Federal affirmative employment programs, compliance with the Uniform Guidelines of Employee Selection Procedures, or other functions vested in the Commission by the President's Reorganization Plan No. 1 of 1978.

7. Disclosure may be made to the National Archives and Record Administration (NARA) and the General Services Administration records management inspections conducted under authority of Title 44 United States Code. NARA is responsible for archiving old records no longer actively used but which may be appropriate for preservation; they are responsible in general for the physical maintenance of the Federal government's records. VA must be able to turn records over to these agencies in order to determine the proper disposition of such records.

8. Disclosure of relevant information may be made to individuals, organizations, private or public agencies, etc., with whom VA has a contract or agreement to perform such services as VA may deem practicable for the purposes of laws administered by VA, in order for the contractor or subcontractor to perform the services of the contract or agreement. VA occasionally contracts out certain functions when this would contribute to effective and efficient operations. VA must be able to give a contractor whatever information is necessary for the contractor to fulfill its duties. In these situations, safeguards are provided in the contract prohibiting the contractor from using or disclosing the information for any purpose other than that described in the contract.

9. Disclosure may be made to a member of Congress or staff person acting for the member when the member or staff person requests the records on behalf of and at the request of an individual. Individuals sometimes request the help of a member of Congress in resolving some issues relating to a matter before VA. The member of Congress then writes VA, and VA must be able to give sufficient information to be responsive to the inquiry.

10. Disclosure may be made to a Federal, State or local agency, upon its official request, to the extent that it is relevant and necessary to that agency's decision regarding: the hiring, retention or transfer of an employee, the issuance of a security clearance, the letting of a contract, or the issuance or continuance of a license, grant or other benefit given by that agency. However, in accordance with an agreement with the U.S. Postal Service, disclosures to the U.S. Postal Service for decisions concerning the employment of veterans will only be made with the Veteran's prior written consent. VA must be able to provide information to agencies conducting background checks on applicants for employment or licensure.

11. VA may disclose information from this system of records to the Department of Justice (DoJ), either on VA's initiative or in response to DoJ's request for the information, after either VA or DoJ determines that such information is relevant to DoJ's representation of the United States or any of its components in legal proceedings before a court or adjudicative body, provided that, in each case, the agency also determines prior to disclosure that release of the records to the DoJ is a use of the information contained in the records that is compatible with the purpose for which VA collected the records. VA, on its own initiative, may disclose records in this system of records in legal proceedings before a court or administrative body after determining that the disclosure of the records to the court or administrative body is a use of the information contained in the records that is compatible with the purpose for which VA collected the records.

12. VA may disclose on its own initiative any information in the system, except the names and home addresses of Veterans and their dependents, that is relevant to a suspected or reasonably imminent violation of the law whether civil, criminal, or regulatory in nature and whether arising by general or program statute or by regulation, rule, or order issued pursuant thereto, to a Federal, State, local, tribal, or foreign agency charged with the responsibility of investigating or prosecuting such violation, or charged with enforcing or implementing the statute, regulation, rule, or order. VA may also disclose on its own initiative the names and addresses of Veterans and their dependents to a Federal agency charged with the responsibility of investigating or prosecuting civil, criminal, or regulatory violations of law, or charged with enforcing or implementing the statute, regulation, or order issued pursuant thereto.

13. Disclosure to other Federal agencies may be made to assist such agencies in preventing and detecting possible fraud or abuse by individuals in their operations and programs.

14. VA may, on its own initiative, disclose any information or records to appropriate agencies, entities, and persons when (1) VA suspects or has confirmed that the integrity or confidentiality of information in the system of records has been compromised; (2) the Department has determined that as a result of the suspected or confirmed compromise, there is a risk of embarrassment or harm to the reputations of the record subjects, harm to economic or property interests, identity theft or fraud, or harm to the security, confidentiality, or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the potentially compromised information; and (3) the disclosure is to agencies, entities, or persons whom VA determines are reasonably necessary to assist or carry out the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm. This routine use permits disclosures by the Department to respond to a suspected or confirmed data breach, including the conduct of any risk analysis or provision of credit protection services as provided in 38 U.S.C. 5724, as the terms are defined in 38 U.S.C. 5727.

DISCLOSURE TO CONSUMER REPORTING AGENCIES:

Pursuant to 5 U.S.C. 552a(b)(12), VA may disclose records from this system to consumer reporting agencies as defined in the Fair Credit Reporting Act (15 US.C. 168la(f)) or the Federal Claims Collection Act of 1966 (31 US.C. 3701(a)(3)).

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:

Records are maintained primarily on a computer disk in a centralized database system. Paper records of program Participation Agreements and individual customer records are maintained in canteen office files.

RETRIEVABILITY:

Records are retrieved by name and/or Social Security number of the participating VA employees or customers.

SAFEGUARDS:

1. Access to VA work and file areas is restricted to VA personnel with a legitimate need for the information in the performance of their official duties. Strict control measures are enforced to ensure that access by these individuals is appropriately limited. Information stored electronically may be accessed by authorized VCS employees at remote locations, including VA health care facilities. Access is controlled by individually unique passwords or codes, which must be changed periodically by the users.

2. Physical access to the Austin VA Data Processing Center is generally restricted to Center employees, custodial personnel, Federal Protective Service, and other security personnel. VA file areas are generally locked after normal duty hours, and the facilities are protected from outside access by the Federal Protective Service or other security personnel. Access to computer rooms is restricted to authorized operational personnel through electronic locking devices. All other persons gaining access to computer rooms are escorted.

3. All data transmissions are encrypted to prevent disclosure of protected Privacy Act information. Access to backup copies of data is restricted to authorized personnel in the same manner as the Austin VA Data Processing Center.

RETENTION AND DISPOSAL:

Records for active participants in the Payroll Deduction Program are maintained indefinitely. Records for participants who leave VA employment voluntarily or involuntarily terminate their participation in the Payroll Deduction Program are retained for three years following the date the account attains a zero balance; or for three years following the date the account balance is written off following unsuccessful collection action.

SYSTEM MANAGER(S) AND ADDRESS:

Official responsible for policies and procedures: Office of the Chief Financial Officer, Veterans Canteen Service (103), Department of Veterans Affairs, 810 Vermont Avenue, NW., Washington, DC 20420. Officials maintaining the system: Chief of the Canteen Service at the facility where the individuals were associated. Addresses for VA facilities are listed in VA Appendix 1.

NOTIFICATION PROCEDURE:

Individuals who wish to determine whether this system of records contains records about them should contact the VCS Payroll Deduction Program Specialist at the Veterans Canteen Service Central Office (VCSCO–FC), St. Louis, Missouri 63125; telephone: (314) 845–1301. Inquiries should include the person's full name, Social Security number, date(s) of contact, and return address.

RECORD ACCESS PROCEDURE:

Individuals seeking information regarding access to and contesting of records in this system may write, call, or visit the VCS Payroll Deduction Program Specialist at the Veterans Canteen Service Central Office (VCSCO–FC), St. Louis, Missouri 63125; telephone: (314) 845–1301.

CONTESTING RECORD PROCEDURES:

(See Record Access Procedures above.)

RECORD SOURCE CATEGORIES:

Information in this system of records is provided by the customers who participate in the program, VA employees and various VA systems.

[FR Doc. 2010–11349 Filed 5–11–10; 8:45 am]

BILLING CODE P