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.

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

STORAGE:

Records are maintained on paper, microfilm, magnetic tape, disk, or laser optical media. In most cases, archival storage of the VistA data to backup tapes are maintained at off-site locations.

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 VA working and storage areas is restricted to VA employees on a "need-to-know" basis. Strict physical security control measures are enforced to ensure that disclosure to these individuals is also based on this same principle. Generally, VA file areas are locked after normal duty hours and the facilities are protected from outside access by the Federal Protective Service or other security personnel.

2. Access to computer rooms at health care facilities and regional data processing centers is generally limited by appropriate locking devices and restricted to authorized VA employees and vendor personnel. Automated Data Processing (ADP) peripheral devices are placed in secure areas (areas that are locked or have limited access) or are otherwise protected. Information in VistA may be accessed by authorized VA employees. Access to file information is controlled at two levels. The systems recognize authorized employees by series of individually unique passwords/codes as a part of each data message, and the employees are limited to only that information in the file which is needed in the performance of their official duties. Information that is downloaded from VistA and maintained on laptops and other approved government equipment is afforded similar storage and access protections as the data that is maintained in the original files. Access to information stored on automated storage media at other VA locations is controlled by individually unique passwords/codes. Access by Office of Inspector General (OIG) staff conducting an audit, investigation, or inspection at the health care facility, or an OIG office location remote from the health care facility, is controlled in the same manner.

3. Information downloaded from VistA and maintained by the OIG headquarters and Field Offices on automated storage media is secured in storage areas for facilities to which only OIG staff have access. Paper documents are similarly secured. Access to paper documents and information on automated storage media is limited to OIG employees who have a need for the information in the performance of their official duties. Access to information stored on automated storage media is controlled by individually unique passwords/codes.

RETENTION AND DISPOSAL:

Paper records and information stored on electronic storage media are maintained and disposed of in accordance with records disposition authority approved by the Archivist of the United States, and VA policies and procedures for media sanitization.

SYSTEM MANAGER(S) AND ADDRESS:

The official responsible for policies and procedures is the Director, Health Data and Informatics (HDI) (19F), Department of Veterans Affairs, 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 the VA facility location at which they are or were employed or made contact. Inquiries should include the person's full name, social security number, dates of employment, 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 VA facility location where they are or were employed or made contact.

CONTESTING RECORD PROCEDURES:

(See Record Access Procedures above.)

RECORD SOURCE CATEGORIES:

Information in this system of records is provided by the individual, supervisors, other employees, personnel records, or obtained from their interaction with the system.

[FR Doc. 2010–1688 Filed 1–26–10; 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 "Disaster Emergency Medical Personnel System (DEMPS)-VA" (98VA104) as set forth in the **Federal Register** 65 FR 25531. VA is amending the system of records by revising the Routine Uses of Records Maintained in the System Including Categories of Users and the Purpose of Such Uses, Retrievability, Systems Manager and Address, and Notification Procedure. 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 February 26, 2010. If no public comment is received, the amended system will become effective February 26, 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: DEMPS is to be used by the Emergency Management Strategic Healthcare Group (EMSHG) primarily in times of national emergencies caused by catastrophic events. This system may be used to respond to internal emergencies occurring within the Veterans Integrated Service Networks (VISNs).

It is the Veterans Health Administration's (VHA) policy to use DEMPS to respond to internal emergencies occurring within the VISNs. In order to provide sufficient health care medical personnel to respond to disasters, it is necessary to develop a nationwide VHA system of special-skilled personnel. These persons would be available to serve for limited periods of time in response to Presidentially-declared and internal VA national emergencies. VHA maintains a nationwide register of clinical personnel who volunteer their special medical skills in response to emergencies.

Information in DEMPS comes from VHA full-time employees who provide the information voluntarily. Information collected and maintained in DEMPS includes personal and demographic information initiated, provided, and authenticated by the employee and contains the necessary approvals and signatures of supervisory officials. Information includes the employee's full name, station and VISN assignment, station address and phone number, home phone number, emergency contact and phone number, professional/job series, grade, specialty, current job assignment, description of advanced degree/certification (if any); physical limitations (if any); prior experience in disaster response (if any); specialized training; related military medical training, other relevant training and dates thereof. DEMPS constitutes a system of records under the Privacy Act of 1974 (5 U.S.C. 552a) and data contained therein are considered private information.

Routine use 7 was amended to disclose information to the National Archives and Records Administration (NARA) and the General Services Administration (GSA) in records management inspections conducted under authority of Title 44, Chapter 29, of the United States Code (U.S.C.). NARA and GSA are responsible for management of old records no longer actively used, but which may be appropriate for preservation, and for the physical maintenance of the Federal government's records. VA must be able to provide the records to NARA and GSA in order to determine the proper disposition of such records.

Routine use 20 was added to disclose information to other Federal agencies that 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 documentation related to or in support of the reported incident.

Routine use 21 was added so that 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.

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.

Dated: December 23, 2009.

John R. Gingrich,

Chief of Staff, Department of Veterans Affairs.

98VA104

SYSTEM NAME:

Disaster Emergency Medical Personnel System (DEMPS)–VA.

SYSTEM LOCATION:

Records are maintained at each of the Department of Veterans Affairs (VA) health care facilities. The address locations for VA facilities were listed in VA Appendix I of the biennial publication of the VA systems of record. Information from these records or copies of records may be maintained at the Department of Veterans Affairs, 810 Vermont Avenue, NW., Washington, DC 20420; Network Directors' Offices; Emergency Management Strategic Healthcare Group Headquarters, VA Medical Center, Martinsburg, WV 25401; or with the Area Emergency Managers located at VA facilities.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

VA employees who make application to VA and are considered for deployment as health care providers primarily in times of national emergencies in response to domestic disasters resulting from natural and technological hazards, terrorist attacks, and the employment of nuclear, biological, and chemical weapons of mass destruction. These individuals may include audiologists, dentists, dietitians, expanded-function dental auxiliaries, licensed practical vocational nurses, nuclear medicine technologists, nurse anesthetists, nurse practitioners, nurses, occupational therapists, optometrists, clinical pharmacists, licensed physical therapists, physician assistants, physicians, podiatrists, psychologists, registered respiratory therapists, certified respiratory therapy technicians, diagnostic and therapeutic radiology technologists, social workers, speech pathologists, contracting specialists, building maintenance, engineering, housekeeping, and other personnel associated with emergency management.

CATEGORIES OF RECORDS IN THE SYSTEM:

Information on VA employees who make application to be deployed as health care providers primarily in times of national emergencies. This source document provides personal and demographic information initiated, provided and authenticated by the employee, and contains the necessary approvals and signatures of officials in the supervisory chain for the employee's

inclusion in the database. Information is provided on a voluntary basis. Information related to identifying and selecting individuals by the Emergency Management Strategic Healthcare Group, networks and medical centers eligible to support specific job tasking and assignments during either disasters internal to the VHA health care system, or external to VHA for which the VA is tasked to provide support under applicable authorities. Requests for issuance of travel orders and necessary reimbursement to VA for subsequent allocation of funds to home stations of deployed personnel are required to cover costs of travel, overtime and other expenses associated with individual deployments. This information is necessary to account for personnel deployed to support disasters, to identify personnel with specific job skills and experience that may be required to support contingency missions tasked to VA under the VA/Department of Defense (DoD) Contingency Plan, and for the development of plans at the corporate, network and medical center level for utilization of VHA personnel in support of VA internal and external disasters.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Authority for maintenance of this system of records is Executive Order 12656 dated November 18, 1988.

PURPOSE(S):

The records may be used for such purpose as to provide information on sufficient health care medical personnel to respond to disasters, to provide information to the Emergency Management Strategic Healthcare Group primarily in times of national emergencies caused by catastrophic events, and to respond to internal emergencies occurring within the Veterans Integrated Service Networks.

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. Selected information (such as name, station and telephone numbers) may be disclosed to other Federal departments and agencies that have an interest in or obligation to track or otherwise audit transfer of funds to VA for reimbursement of tasks.

2. Statistical information and other data may be disclosed to Federal, State and local government agencies to assist in disaster planning and after-action reports.

3. When a record on its face, or in conjunction with other records, indicates a violation or potential violation of law, whether civil, criminal or regulatory in nature, and whether arising by general statute or particular program statute, or by regulation, rule or order issued pursuant thereto, disclosure may be made to the appropriate agency, whether Federal, foreign, State, local, or tribal, or other public authority responsible for enforcing, investigating or prosecuting such violation or charged with enforcing or implementing the statute, or rule, regulation, or order issued pursuant thereto, if the information disclosed is relevant to any enforcement, regulatory, investigative or prosecutive responsibility of the receiving entity.

4. Disclosure may be made to any source, such as a police department or the Federal Bureau of Investigation, from which additional information is requested to the extent necessary to identify the individual, inform the source of the purpose(s) of the request, and to identify the type of information requested such as DEMPS personnel present at a crime scene caused by terrorists.

5. Disclosure may be made to an agency in the executive, legislative, or judicial branch, or the District of Columbia Government in response to its request, or at the initiation of VA, for information in connection with the selection of an employee for the deployment and future training of an individual, the letting of a contract, the issuance of a license, grant, or other benefits by the requesting agency, or the lawful statutory, administrative, or investigative purpose of the agency to the extent that the information is relevant and necessary to the requesting agency's deployment/Federal Response Framework needs.

6. Disclosure may be made to a Member of Congress or to a congressional staff member in response to an inquiry of the congressional office made at the written request of the constituent about whom the record is maintained.

7. Disclosure may be made to the National Archives and Records Administration (NARA) and the General Services Administration (GSA) in records management inspections conducted under authority of 44 U.S.C. 2904 and 2906.

8. Disclosure may be made to a Federal agency or to a State or local government licensing board, or to the Federation of State Medical Boards, or a similar non-government entity, provided the entity maintains records concerning individuals' employment histories, is engaged in the issuance, retention or revocation of licenses, certifications, or registration necessary to practice an occupation, profession or specialty. The disclosure is for the Department to obtain information relevant to a Department decision concerning the hiring, retention or termination of an employee, or to inform a Federal agency, licensing boards or to the appropriate non-government entities about the health care practices of a terminated, resigned, or retired health care employee whose professional health care activity so significantly failed to conform to generally accepted standards of professional medical practice as to raise reasonable concern for the health and safety of patients receiving medical care in the private sector or from another Federal agency. These records may also be disclosed as part of an ongoing computer matching program to accomplish these purposes.

9. Information may be disclosed to private sector (*i.e.*, non-Federal, State, or local governments) agencies, organizations, boards, bureaus, or commissions (*e.g.*, The Joint Commission) when the disclosure is in the best interest of the government (*e.g.*, to obtain accreditation or other approval rating). When cooperation with the private sector entity, through the exchange of individual records, directly benefits VA's completion of its mission, enhances personnel management functions, or increases the public confidence in VA's or the Federal government's role in the community, then the government's best interests are served. Further, only such information that is clearly relevant and necessary for accomplishing the intended uses of the information as certified by the receiving private sector entity is to be furnished.

10. Information may be disclosed to a State or local government entity or national certifying body that has the authority to make decisions concerning the issuance, retention or revocation of licenses.

11. Information may be disclosed to the Department of Justice and United States Attorneys in defense or prosecution of litigation involving the United States, and to Federal agencies upon their request in connection with

review of administrative tort claims filed under the Federal Tort Claims Act, 28 U.S.C. 2672.

12. Information on deployment to Federal/VHA emergencies, performance, or other personnel-related material may be disclosed to any facility with which there is, or there is proposed to be, an affiliation, sharing agreement, contract, or similar arrangement, for purposes of establishing, maintaining, or expanding any such relationship.

13. Information concerning a health care provider's professional qualifications and clinical privileges may be disclosed to a VA/emergency disaster-served client patient, or the representative or guardian of a patient who, due to physical or mental incapacity, lacks sufficient understanding or legal capacity to make decisions concerning his or her medical care, who is receiving or contemplating receiving medical or other patient care services from the provider when the information is needed by the patient or the patient's representative or guardian in order to make a decision related to the initiation of treatment, continuation or discontinuation of treatment, or receiving a specific treatment that is proposed or planned by the provider. Disclosure will be limited to information concerning the health care provider's professional qualifications (professional education, training and current licensure/certification status), professional employment history, and current clinical privileges.

14. Information may be disclosed 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.

15. Information may be disclosed to the VA-appointed representative of an employee of all notices, determinations, decisions, or other written communications issued to the employee in connection with an examination ordered by VA under medical evaluation (formerly fitness-for-duty) examination procedures or Department-filed disability retirement procedures.

16. Information may be disclosed 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.

17. Information may be disclosed 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.

18. Information may be disclosed to the Federal Labor Relations Authority (including its General Counsel) when requested in connection with investigation and resolution of allegations of unfair labor practices, and in connection with the resolution of exceptions to arbitrator awards when a question of material fact is raised.

19. Disclosure may be made to agency contractors, grantees, or volunteers who have been engaged to assist the agency in the performance of a contract service, grant, cooperative agreement, or other activity related to this system of records and who need to have access to the records in order to perform the activity. Recipients shall be required to comply with the requirement of the Privacy Act of 1974, as amended, 5 U.S.C. 552a.

20. 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.

21. 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:

Reports of all transactions dealing with data will be used within VA and will not be provided to any consumer-reporting agency.

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

STORAGE:

Automated records are maintained at all levels of management outlined in system location. Automated information may be stored on microfilm, magnetic tape, disk, or databases.

RETRIEVABILITY:

Records are retrieved from the system by the name, professional title, VISN, home station, professional specialty, job position title, etc., of the individuals on whom they are maintained.

SAFEGUARDS:

1. Access to VA working and storage areas in VA health care facilities is restricted to VA employees on a need-to-know basis; strict control measures are enforced to ensure that disclosure to these individuals is also based on this same principle. Generally, VA file areas are locked after normal duty hours, and the health care facilities are protected from outside access by the Federal Protective Service or other security personnel.

2. Access to the Veterans Health Information Systems Technology Architecture (VistA) computer room within the health care facilities is generally limited by appropriate security devices and restricted to authorized VA employees and vendor personnel. Automatic Data Processing (ADP) peripheral devices are generally placed in secure areas (areas that are locked or have limited access) or are otherwise protected. Authorized VA employees may access information in the VistA system. Access to file information is controlled at two levels: The system recognizes authorized employees by a series of individually unique passwords/codes as a part of each data message, and the employees are limited to only that information in the file which is needed in the performance of their official duties.

RETENTION AND DISPOSAL:

An automated database of DEMPS personnel will be maintained at the employing VA facility. If the individual transfers to another VA facility location, the name will be added to the database at the new location. Information stored

on electronic storage media is maintained and disposed of in accordance with the records disposition authority approved by the Archivist of the United States.

SYSTEM MANAGER(S) AND ADDRESS:

Official responsible for maintaining the system: Director, Emergency Management Strategic Healthcare Group (EMSHG) (13C), VA Medical Center, Martinsburg, West Virginia, 25401.

NOTIFICATION PROCEDURE:

Individuals who wish to determine whether this system of records contains information about them should contact the VA facility location at which they made application as a deployment volunteer, or are or were employed. Inquiries should include the employee's full name, date of application for employment or dates of employment, 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 VA facility location where they made application for employment or are or were employed.

CONTESTING RECORD PROCEDURES:

(*See* Record Access Procedures above.)

RECORD SOURCE CATEGORIES:

The information will be provided by the individual VA employee and the VA medical facility (home station) or other VA location at which the employee was employed. EMSHG Headquarters will also provide information for updates of deployment status and availability.

[FR Doc. 2010–1689 Filed 1–26–10; 8:45 am]

BILLING CODE 8320–01–P