

Authority: Congress created the U.S.-China Economic and Security Review Commission in 2000 in the National Defense Authorization Act (Pub. L. 106-398), as amended by Division P of the Consolidated Appropriations Resolution, 2003 (Pub. L. 108-7), as amended by Public Law 109-108 (November 22, 2005).

Dated: May 5, 2009.

Kathleen J. Michels,

Associate Director, U.S.-China Economic and Security Review Commission.

[FR Doc. E9-10759 Filed 5-7-09; 8:45 am]

BILLING CODE 1137-00-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 "Telephone Service for Clinical Care Records-VA" (113VA112) as set forth in the **Federal Register** 67 FR 63497. VA is amending the system of records by revising the System Name, Routine Uses of Records Maintained in the System Including Categories of Users and the Purpose of Such Uses, Storage, Safeguards, and System Manager and Address. 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 8, 2009. If no public comment is received, the amended system will become effective June 8, 2009.

ADDRESSES: Written comments may be submitted through 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 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:

I. Description of Proposed System of Records

The primary purpose of telephone care and service function is to provide veterans with clinical advice and education related to symptoms or problems an enrolled veteran caller may be experiencing. Calls may be made by family members but records of the calls will be maintained in the enrolled veteran's record. Except in the case of emergencies, clinical advice and education may only be provided to enrolled veterans. In order to better track and retrieve information about previous calls, all records of calls will be maintained under the name of the enrolled veteran. Records will not be retrievable by the name of the caller. Telephone care and service provides another mode of access for veterans that is available 24 hours a day, seven days a week from any place in the country. The telephone care function acts as a part of the primary and ambulatory care delivery system and augments that system by providing advice to callers over the telephone. When patients or family members call with a concern or request, a record of the call is developed, whether it is a clinical or administrative issue.

Clinical symptom calls are managed through the use of pre-approved clinical algorithms that ask a series of questions and based on the answers to each question moves to the next question, which eventually leads to the advice that is to be provided to the caller. The record of the call captures the questions asked, answers given, particularly those answers that reflect something abnormal, and the advice provided. Documentation of this type of information is consistent with standard requirements for medical record documentation, which captures symptoms and findings as they relate to how specific questions are answered and a plan of action established. This information is also recorded in the patient's medical record. At a minimum, documentation includes the complaint(s) and symptoms of the enrolled veteran, the algorithm and/or protocol used and the advice given. Information is recorded either electronically in the progress notes of the medical record and in the Call Center database. Acting as a part of the

primary and ambulatory care delivery system, the telephone care function may provide private sector providers or facilities with relevant clinical information about enrolled veterans in urgent or emergent situations. Information such as allergies, results of recent lab tests, medications, recent health history or procedures may be provided. Telephone care and service for clinical symptom calls are provided in a number of ways, including contracts with private sector vendors, contracts with VA facilities or Networks that have developed clinical Call Centers, or through medical center-based Call Centers in primary care and other types of clinics. A number of VA facilities and Networks are providing access to telephone care and service through clinics or medical center-based Call Centers during the day and through Network or contracted Call Centers during non-administrative hours. Protocols or algorithms are used at any of these sites when advice is given by a registered nurse without first consulting with a clinician and all of these calls must be documented in the medical record and Call Center database. Keeping records of all calls to a clinical Call Center in a separate database is the standard of practice for clinical Call Centers and is a required accreditation standard of the Utilization Review Accreditation Commission (URAC) for clinical Call Centers. Accreditation by URAC or another clinical Call Center accrediting body, if one should become available, is required for Regional or VISN call centers by the VHA Directive 2007-033 Telephone Service for Clinical Care. This system allows a record of all previous calls made by or for a veteran to be accessed whenever patients or family members call, which improves both the quality and the timeliness of addressing callers' concerns. Records are generally collected and stored electronically for ease of retrieval by the veteran's name or other personal identifier. The primary purpose of the data in this system of records is for rapid retrieval and ease of access to a record of all calls made by or for veterans, including the complaints of the patient, the findings according to the algorithms and the advice provided. This information is also used for follow-up calls to some patients. Information is also used for aggregation of data for the purposes of monitoring and improving quality. Though information is retrievable by individual patient identifier, when reporting aggregate information for purposes, such as quality, patient identifiers are not

provided. Access to such records provide Call Center staff with information about previous contacts and the clinical symptoms reported by veterans in those contacts. The protocol used, education provided, advice given and actions taken by the caller in previous calls are readily available to Call Center staff each time a veteran or family member calls, which improves the quality of the services. Access to patient-specific information located in Call Center databases and storage areas is restricted to VA employees and contract personnel 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 Call Center file areas are locked after normal duty hours or when the Call Center is closed and the facilities are protected from outside access by the Federal Protective Service or other security personnel. VA and contracted Call Centers are held to the Department of Veterans Affairs Computer Security Policy and all free standing and contracted Call Centers are required to develop and implement a Computer Security Policy that is consistent with the National Policy. Call Centers located within a medical center are required to meet the requirements of that medical center's computer security policy. Access to VA and contracted Call Centers and computer rooms is generally limited by appropriate locking devices and restricted to authorized VA employees and vendor personnel. Information in the Veterans Health Information Systems and Technology Architecture (VistA) may be accessed by authorized VA employees or authorized contract employees. Access to file information is controlled at two levels; the systems recognize authorized employees or contract employees by a series of individually unique passwords/codes as a part of each data message, and personnel 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 VA databases 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 and contract locations is controlled by individually unique passwords/codes. Remote access to VHA information in VistA is provided to those Call Center employees, either VA or contract staff, that require access to information stored in the medical record. Access to this information is protected through

hardened user access and is controlled by individual unique passwords. Additionally, contracted Call Centers, either VA or private sector, are required to have a separate computer security plan that meets national information security requirements.

II. Compatibility of the Proposed Routine Uses

The Report of Intent to Amend a System of 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.

Routine use 14 was added to disclose information to the National Archives and Record 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 15 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/or documentation related to or in support of the reported incident.

Routine use 16 was added so that the 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.

Approved: April 21, 2009.

John R. Gingrich,

Chief of Staff, Department of Veterans Affairs.

113VA112

SYSTEM NAME:

Telephone Service for Clinical Care Records—VA.

SYSTEM LOCATION:

Records are located at each Call Center, which are operated at VA health care facilities or at contractor locations. Address locations for VA facilities are listed in VA Appendix 1 of the biennial publication of VA Privacy Act Issuances. In addition, information from clinical symptom calls is maintained in the patient's medical record at VA health care facilities and at the Department of Veterans Affairs (VA), 810 Vermont Avenue, NW., Washington, DC; Veterans Integrated Service Network Offices (VISNs); and Employee Education Systems.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

The records include information concerning individual enrolled patients.

CATEGORIES OF RECORDS IN THE SYSTEM:

The records may include information related to:

1. Clinical care such as clinical symptoms, questions asked about symptoms, answers received, clinical protocol used and advice provided. It might include doctors' orders for patient care including nursing care, current medications, including their scheduling and delivery, consultations, radiology, laboratory and other diagnostic and therapeutic examinations and results; clinical protocol and other reference materials; education provided, including title of education material and reports of contact with individuals or groups. It includes information related to the patient's or family member's understanding of the advice given and their plan of action and, sometimes, the effectiveness of those actions.

2. Record of all calls made to the Call Center, including caller questions about medications, their uses and side effects; requests for renewals of prescriptions, appointment changes, benefits information and the actions taken related to each call, including the notification of providers and other staffs about the call.

3. Contact information from private sector medical facilities or clinicians contacting the VA about issues such as enrolled veterans' visits to an emergency department or admissions to a community medical center.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Title 38, United States Code, section 501.

PURPOSE(S):

The purpose of these records is to provide clinical and administrative support to patient care and provide medical and administrative documentation of the care and/or services provided in Call Centers. The records may be used for such purposes as improving Call Center staff's ability to provide telephone care services to veterans and the quality of the service by having immediate access to records of calls made previously by the veteran. Records may be used for purposes of notifying VA providers of the patient's condition and status, the criteria used to judge the status of the patient and/or the information given to the external provider on follow-up steps that they must take to receive authorization for the care. Records may be used to assess and improve the quality of the services provided through telephone care services and to produce various management and patient follow-up reports. Records may be used to respond to patient, family and other inquiries, including at times non-VA clinicians and Joint Commission for Accreditation of Healthcare Organizations (JCAHO) or the Utilization Review Accreditation Commission (URAC) for the accreditation of a Call Center or facility. Records may also be used to conduct health care related studies, statistical analysis, and resource allocation planning using data that has been stripped of individual patient identifiers. The clinical information is integrated into the patient's overall medical record, into quality improvement plans, and activities of the facility, such as utilization review and risk management. They are also used to improve Call Center services, such as patient education, the improved integration of clinical care, the provision of telephone care services, and communication.

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. 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 that individual.

2. Disclosure may be made 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.

3. Disclosure may be made to a Federal agency or to a State or local government licensing board and/or to the Federation of State Medical Boards or a similar non-government entity which maintains records concerning individual's employment histories or concerning the issuance, retention or revocation of licenses, certifications, or registration necessary to practice an occupation, profession or specialty, in order 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 or licensing boards or 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.

4. Disclosure may be made for program review purposes and the seeking of accreditation and/or certification, disclosure may be made to survey teams of the Joint Commission on Accreditation of Healthcare

Organizations, College of American Pathologists, American Association of Blood Banks, and similar national accreditation agencies or boards with whom VA has a contract or agreement to conduct such reviews, but only to the extent that the information is necessary and relevant to the review.

5. Disclosure may be made to a State or local government entity or national certifying body which has the authority to make decisions concerning the issuance, retention or revocation of licenses, certifications or registrations required to practice a health care profession, when requested in writing by an investigator or supervisory official of the licensing entity or national certifying body for the purpose of making a decision concerning the issuance, retention or revocation of the license, certification or registration of a named health care professional.

6. Disclosure may be made to the National Practitioner Data Bank at the time of hiring and/or clinical privileging/reprivileging of health care practitioners, and other times as deemed necessary by VA.

7. Disclosure may be made to the National Practitioner Data Bank and/or State Licensing Board in the State(s) in which a practitioner is licensed, in which the VA facility is located, and/or in which an act or omission occurred upon which a medical malpractice claim was based when VA reports information concerning: (1) Any payment for the benefit of a physician, dentist, or other licensed health care practitioner which was made as the result of a settlement or judgment of a claim of medical malpractice if an appropriate determination is made in accordance with agency policy that payment was related to substandard care, professional incompetence or professional misconduct on the part of the individual; (2) a final decision which relates to possible incompetence or improper professional conduct that adversely affects the clinical privileges of a physician or dentist for a period longer than 30 days; or, (3) the acceptance of the surrender of clinical privileges or any restriction of such privileges by a physician or dentist either while under investigation by the health care entity relating to possible incompetence or improper professional conduct, or in return for not conducting such an investigation or proceeding. These records may also be disclosed as part of a computer matching program to accomplish these purposes.

8. Disclosure of information related to the performance of a health care student or provider may be made to a medical or nursing school or other health care

related training institution or other facility with which there is an affiliation, sharing agreement, contract or similar arrangement when the student or provider is enrolled at or employed by the school or training institution or other facility and the information is needed for personnel management, rating and/or evaluation purposes.

9. 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.

10. Disclosure may be made to a Federal agency, in response to its request, in connection with the hiring or retention of an employee, the issuance of a security clearance, reporting of an investigation of an employee, the letting of a contract, or the issuance or continuance of a license, grant or other benefit given by that agency to the extent that the information is relevant and necessary to the requesting agency's decision on the matter.

11. Disclosure of information may be made to the next-of-kin and/or the person(s) with whom the patient has a meaningful relationship to the extent necessary and on a need-to-know basis consistent with good medical-ethical practices.

12. On its own initiative, VA may disclose information, except for the names and home addresses of veterans and their dependents, to a Federal, State, local, tribal or foreign 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, rule or order issued pursuant thereto. On its own initiative, VA may also disclose 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, rule or order issued pursuant thereto.

13. Disclosure of relevant information may be made to a non-VA physician or medical facility staff caring for a veteran for the purpose of providing relevant clinical information in an urgent or emergent situation.

14. 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 Title 44, Chapter 29, of the United States Code (U.S.C.).

15. 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.

16. 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.

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

STORAGE:

Records are maintained in the electronic medical record and on an automated storage media, such as magnetic tape, disc or laser optical media.

RETRIEVABILITY:

Records are retrieved by name, social security number or other assigned identifier of the enrolled veteran who is calling or about whom the call is being made.

SAFEGUARDS:

1. Access to patient-specific information located in Call Center databases and storage areas is restricted to VA employees and contract personnel 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 Call Center areas are locked after normal duty hours or when the Call Center is closed, and the facilities are protected from outside access by the Federal Protective Service or other security personnel.

2. Access to VA and contracted Call Centers and computer rooms is generally limited by appropriate locking devices and restricted to authorized VA employees and vendor personnel. Information in the Veterans Health Information Systems and Technology Architecture (Vista) may be accessed by authorized VA employees or authorized contract employees. Access to file information is controlled at two levels; the systems recognize authorized employees or contract employees by a series of individually unique passwords/codes as a part of each data message, and personnel 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 VA 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 and contract locations is controlled by individually unique passwords/codes.

3. Remote access to VHA information in Vista is provided to those Call Center employees, either VA or contract staff, that require access to information stored in the medical record. Access to this information is protected through hardened user access and is controlled by individual unique passwords. Additionally, contracted Call Centers, either VA or private sector, are required to have a separate computer security plan that meets national information security requirements.

RETENTION AND DISPOSAL:

Records are to be disposed of in accordance with the Veterans Health Administration Records Control Schedule; 10-1. Paper records and information stored on electronic storage media are 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 policies and procedures: Chief Consultant for Primary Care (11PC) Department of Veterans Affairs, 810 Vermont Avenue, NW., Washington, DC 20420. Officials maintaining the system: Network and/or facility director at the Network and/or

facility where the individuals are associated.

NOTIFICATION PROCEDURE:

Individuals who wish to determine whether a record is being maintained in this system under his or her name or other personal identifier, or wants to determine the contents of such record, should submit a written request or apply in person to the last VA health care facility where care was rendered. Addresses of VA health care facilities may be found at <http://www2.va.gov/directory/guide/home.asp?isFlash=1>. 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 or visit the VA facility location where they normally receive their care.

CONTESTING RECORD PROCEDURES:

(See Record Access Procedures above.)

RECORD SOURCE CATEGORIES:

Record sources include: enrolled patients, patients' families and friends, private medical facilities and their clinical and administrative staffs, health care professionals, Patient Medical Records—VA (24VA136), VistA (79VA19), VA health care providers, and Call Center nurses and administrative staff.

[FR Doc. E9-10711 Filed 5-7-09; 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 "National Chaplain Management Information System (NCMIS)—VA" (84VA111K) as set forth in the **Federal Register** 59 FR 13765 and last amended in the **Federal Register** on March 23, 1994. 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. 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 8, 2009. If no public comment is received, the amended system will become effective June 8, 2009.

ADDRESSES: Written comments may be submitted through 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 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:

Chaplain Service of the Veterans Health Administration, Department of Veterans Affairs, has developed a data base to maintain information that will be used as part of a comprehensive program to evaluate applicants for employment as chaplains, and to plan the Spiritual and Pastoral Care Program. The information will be used to facilitate personnel succession planning. It will also support the documentation and tracking of credentialing and privileging for all chaplains providing patient care in the system.

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.

Routine Use 13 was added to disclose relevant information that may be made to individuals, organizations, private or public agencies, or other entities with whom VA has a contract or agreement or where there is a subcontract to

perform such service 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.

Routine use 14 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.

Routine use 15 was added so that the 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.

Approved: April 21, 2009.

John R. Gingrich,

Chief of Staff, Department of Veterans Affairs.

84VA111K

SYSTEM NAME:

"National Chaplain Management Information System (NCMIS)—VA."

SYSTEM LOCATION:

The data base will reside on its own micro-computers at the National VA Chaplain Center (301/111K) at the Department of Veterans Affairs (VA) Medical Center (VAMC) located at 100 Emancipation Road, Hampton, Virginia 23667.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

The personal data collected will be limited to VA Chaplains, other VA