

that national security could be threatened.

SYSTEM MANAGER AND ADDRESS:

Deputy Director, Individual Assistance, Disaster Assistance Directorate, Federal Emergency Management Agency, 500 C Street, SW., Washington, DC 20472.

NOTIFICATION PROCEDURE:

Individuals seeking notification of and access to any record contained in this system of records, or seeking to contest its content, may submit a request in writing to FEMA's FOIA Officer, 500 C Street, SW., Attn: FOIA Coordinator, Washington, DC 20472.

When seeking records about yourself from this system of records or any other Departmental system of records your request must conform with the Privacy Act regulations set forth in 6 CFR part 5. You must first verify your identity, meaning that you must provide your full name, current address and date and place of birth. You must sign your request, and your signature must either be notarized or submitted under 28 U.S.C. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, you may obtain forms for this purpose from the Chief Privacy Officer and Chief Freedom of Information Act Officer, <http://www.dhs.gov> or 1-866-431-0486. In addition you should provide the following:

- An explanation of why you believe the Department would have information on you;
- Identify which component(s) of the Department you believe may have the information about you;
- Specify when you believe the records would have been created;
- Provide any other information that will help the FOIA staff determine which DHS component agency may have responsive records; and
- If your request is seeking records pertaining to another living individual, you must include a statement from that individual certifying his/her agreement for you to access his/her records.

Without this bulleted information the component(s) may not be able to conduct an effective search, and your request may be denied due to lack of specificity or lack of compliance with applicable regulations.

RECORD ACCESS PROCEDURES:

See "Notification procedure" above.

CONTESTING RECORD PROCEDURES:

See "Notification procedure" above.

RECORD SOURCE CATEGORIES:

Records are obtained from registrants of NEFRS and individuals searching NEFRS, LEOs, and the third party authentication service indicating an individual has been approved or not approved.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

Dated: July 25, 2011.

Mary Ellen Callahan,
Chief Privacy Officer, Department of Homeland Security.

[FR Doc. 2011-22167 Filed 8-29-11; 8:45 am]

BILLING CODE 9110-17-P

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS-2011-0081]

Privacy Act of 1974; Department of Homeland Security ALL-034 Emergency Care Medical Records System of Records Notice

AGENCY: Privacy Office, DHS.

ACTION: Notice of Privacy Act system of records.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Homeland Security proposes to establish a new Department of Homeland Security system of records titled, "Department of Homeland Security/ALL-034 Emergency Care Medical Records System of Records Notice." This system of records will allow the Department of Homeland Security Office of Health Affairs to collect and maintain records on individuals who receive emergency care from Department Emergency Medical Services providers. Individuals in this system include anyone who experiences a medical emergency and is treated by an on-duty Departmental Emergency Medical Services medical care provider. This newly established system will be included in the Department of Homeland Security's inventory of record systems.

DATES: Submit comments on or before September 29, 2011. This new system will be effective September 29, 2011.

ADDRESSES: You may submit comments, identified by docket number DHS-2011-0081 by one of the following methods:

- *Federal e-Rulemaking Portal:* <http://www.regulations.gov>. Follow the instructions for submitting comments.
- *Fax:* 703-483-2999.
- *Mail:* Mary Ellen Callahan, Chief Privacy Officer, Privacy Office,

Department of Homeland Security, Washington, DC 20528.

• *Instructions:* All submissions received must include the agency name and docket number for this rulemaking. All comments received will be posted without change to <http://www.regulations.gov>, including any personal information provided.

• *Docket:* For access to the docket to read background documents or comments received go to <http://www.regulations.gov>.

FOR FURTHER INFORMATION CONTACT: For questions please contact: Mary Ellen Callahan (703-235-0780), Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 20528.

SUPPLEMENTARY INFORMATION:

I. Background

In accordance with the Privacy Act of 1974, 5 U.S.C. 552a, the Department of Homeland Security (DHS) Office of Health Affairs (OHA) proposes to establish a new DHS system of records titled, "DHS/ALL-034 Emergency Care Medical Records."

The Assistant Secretary for Health Affairs and Chief Medical Officer (ASHA/CMO) exercises oversight over all medical and public health activities of DHS, with the exception of U.S. Coast Guard (USCG) medical and public health activities. Throughout its components, the DHS workforce includes approximately 3,500 Emergency Medical Service (EMS) healthcare providers rendering emergency medical care in the pre-hospital environment, primarily to DHS employees and, when necessary, to individuals encountered in the course of duty in need of emergency care. These DHS EMS healthcare providers are employed by the following DHS components: U.S. Customs and Border Protection (CBP), U.S. Immigration and Customs Enforcement (ICE), the United States Secret Service (USSS), Transportation Security Administration (TSA), U.S. Citizenship and Immigration Services (USCIS), Federal Law Enforcement Training Center (FLETC), Federal Emergency Management Agency (FEMA), and Science & Technology Directorate (S&T).

OHA administers oversight of DHS EMS healthcare providers through its Medical Quality Management (MQM) program, to ensure DHS EMS providers deliver consistent, quality medical care. To support MQM, OHA operates the electronic Patient Care Record (ePCR), an electronic encounter-based database designed for EMS management. After administering emergency care, DHS

EMS medical care providers manually enter emergency medical care information into ePCR. ePCR captures all aspects of patient care, from the initial dispatch of a vehicle and personnel to a designated site, demographics, vital signs (initial assessment), treatment, and transfer of care and/or patient transport. The system captures patient data such as name, date of birth, and medical information. Concurrent with the publication of this notice, DHS is publishing a Privacy Impact Assessment (PIA) describing the ePCR system. This PIA will be available at the DHS Privacy Office Web site at <http://www.dhs.gov/privacy>. ePCR improves MQM at the Department by allowing OHA to track and trend data quality, including documentation review, clinical performance, and performance improvement initiatives. This system assists OHA in assessing overall quality of care provided while ensuring that a high standard of care is continually met.

This includes electronic data in ePCR operated by OHA as well as those same EMS encounter records when kept by the EMS provider, in paper form. Individuals covered by this system include members of the public who are treated by on-duty DHS Emergency Medical Services (EMS) healthcare provider. When patients are DHS or other federal employees, their records are considered part of the OPM/GOVT-10—Employee Medical File System Records, 71 FR 3560 (Jun. 19, 2006.) When patients are not Federal employees, such as members of the public, their records are considered part of this system.

OHA has primary responsibility within the Department for “ensuring internal and external coordination of all medical preparedness and response activities of the Department, including training, exercises, and equipment support.” See Section 516(c)(3) of the Post Katrina Emergency Management and Reform Act, Public Law 109–295, 6 U.S.C. 321e(c). In addition, the Secretary has delegated to OHA responsibility for providing oversight for all medical and health activities of the Department. See DHS Delegation to the Assistant Secretary of Health Affairs and Chief Medical Officer, No. 5001 (signed July 28, 2008). As per internal DHS directive, OHA ensures the MQM program is appropriately implemented within the department and that health care service standards are consistently applied across the department. This includes exercising oversight for development of quality assurance activities (quality improvement, risk management documentation, and

medical record management) within DHS. The responsibility of MQM necessitates a patient care reporting system to gather records of pre-hospital emergency medical care rendered by DHS employees, as part of their official DHS duties.

Due to the sensitive and private nature of patient medical records, ePCR has been evaluated to identify risks and corresponding mitigation strategies. Risks may include unauthorized disclosures, incorrect data entry, software viruses, unauthorized access to the system, sharing of data with private sector entities, and data security breaches. Mitigation activities involve privacy and security awareness training for all users, enforcement of role-based access to varied aspects of ePCR (e.g., end-users have access only to their component-specific patient data and any other patient encounter reports for which they have been identified as providing care).

Designated persons (Component Medical Director, Component EMS Coordinators, and ePCR Administrator) within the components will have full administrative review access to all records for quality assurance purposes. The OHA Medical Quality Management Branch and the OHA Medical First Responder Coordination Branch will have rights to run ad hoc reports and query data as it relates to quality assurance tracking and trending indicators (completeness of record, adherence to standards of care/protocols and training) on all component data. Audit logs are periodically reviewed for inconsistencies. Any inconsistencies are immediately addressed through the Component Medical Director, EMS coordinators, or Component Information Technology (IT) and Security Compliance Officer to correct or resolve any issues and concerns. The purpose of ePCR is to support OHA’s MQM program, and this purpose is supported by routine uses for sharing this data for notification of medical hazard, worker’s compensation claims, through formal legal channels, and other limited administrative purposes.

This newly established system will be included in DHS’s inventory of record systems.

II. Privacy Act

The Privacy Act embodies fair information practice principles in a statutory framework governing the means by which the U.S. Government collects, maintains, uses, and disseminates individuals’ records. The Privacy Act applies to information that is maintained in a “system of records.” A “system of records” is a group of any

records under the control of an agency for which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined to encompass U.S. citizens and lawful permanent residents. As a matter of policy, DHS extends administrative Privacy Act protections to all individuals where systems of records maintain information on U.S. citizens, lawful permanent residents, and visitors.

Below is the description of the DHS/OHA-002 Emergency Care Medical Records System of Records.

In accordance with 5 U.S.C. 552a(r), DHS has provided a report of this system of records to the Office of Management and Budget and to Congress.

III. Health Insurance Portability and Accountability Act

For this collection of health information, OHA and participating components are not subject to the provisions of the Health Insurance Portability and Accountability Act (HIPAA) of 1996 regulation, “Standards for Privacy of Individually Identifiable Health Information” (Privacy Rule), 45 CFR parts 160 and 164. OHA does not meet the statutory definition of a covered entity under HIPAA, 42 U.S.C. 1320d–1. Because OHA and participating components are not a covered entity, the restrictions prescribed by the HIPAA Privacy Rule are not applicable.

SYSTEM OF RECORDS

**Department of Homeland Security (DHS)/
Office of Health Affairs (OHA)—002
Emergency Care Medical Records (ECMR)**

SYSTEM NAME:

DHS/OHA—002 Emergency Care Medical Records.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

Records are maintained in the electronic Patient Care Record (ePCR) system at the OHA Headquarters in Washington, DC.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Individuals covered by this system include members of the public, including federal contractors, who are treated by an on-duty DHS Emergency Medical Services (EMS) healthcare provider. When patients are DHS or other federal employees, their records are considered part of the OPM/GOVT–

10—Employee Medical File System Records, 71 FR 35360 (Jun. 19, 2006.)

CATEGORIES OF RECORDS IN THE SYSTEM:

- Patient name.
- Patient case/identification number (not Social Security Number).
- Account of the illness or injury.
- Date of birth and age.
- Gender.
- Location.
- Address (residential or business, if/ as relevant).
- Type of injury.
- Current medications.
- Allergies.
- Past medical history.
- Assessment of injury.
- Chief complaint.
- Vital signs.
- Treatment provided and/or procedures.
- Transfer of care, refusal of care, and/or transportation mode and destination.
- Medication dispensed.
- Discharge instructions for follow-on care.
- If necessary, patient's guardian or legal representative.
- Patient's health insurance information, if any.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

OHA has primary responsibility within the Department for "ensuring internal and external coordination of all medical preparedness and response activities of the Department, including training, exercises, and equipment support." See Section 516(c)(3) of the Post Katrina Emergency Management and Reform Act, Pub. L. 109–295, 6 U.S.C. 321e(c). In addition, the Secretary has delegated to OHA responsibility for providing oversight for all medical and health activities of the Department. See DHS Delegation to the Assistant Secretary of Health Affairs and Chief Medical Officer, No. 5001 (signed July 28, 2008). As per internal DHS directive, OHA ensures the MQM program is appropriately implemented within the department and that health care service standards are consistently applied across the department. This includes exercising oversight for development of quality assurance activities (quality improvement, risk management documentation, and medical record management) within DHS. The responsibility of MQM necessitates a patient care reporting system to gather records of pre-hospital emergency medical care rendered by DHS employees, as part of their official DHS duties.

PURPOSE(S):

The purpose of this system is to support MQM oversight to ensure

consistent quality medical care and standardize the documentation of care rendered by DHS EMS medical care providers in diverse environments.

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

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside DHS as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

A. To the Department of Justice (DOJ), including U.S. Attorney Offices, or other federal agency conducting litigation or in proceedings before any court, adjudicative or administrative body, when it is necessary to the litigation and one of the following is a party to the litigation or has an interest in such litigation:

1. DHS or any component thereof;
2. Any employee of DHS in his/her official capacity;
3. Any employee of DHS in his/her individual capacity where DOJ or DHS has agreed to represent the employee; or
4. The U.S. or any agency thereof, is a party to the litigation or has an interest in such litigation, and DHS determines that the records are both relevant and necessary to the litigation and the use of such records is compatible with the purpose for which DHS collected the records.

B. To a congressional office from the record of an individual in response to an inquiry from that congressional office made at the request of the individual to whom the record pertains.

C. To the National Archives and Records Administration (NARA) or other federal government agencies pursuant to records management inspections being conducted under the authority of 44 U.S.C. 2904 and 2906.

D. To an agency, organization, or individual for the purpose of performing audit or oversight operations as authorized by law, but only such information as is necessary and relevant to such audit or oversight function.

E. To appropriate agencies, entities, and persons when:

1. DHS suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised;

2. DHS has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by

DHS or another agency or entity) or harm to the individual that rely upon the compromised information; and

3. The disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with DHS's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

F. To contractors and their agents, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for DHS, when necessary to accomplish an agency function related to this system of records. Individuals provided information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure as are applicable to DHS officers and employees.

G. To appropriate federal, State, local, tribal, or foreign governmental agencies or multilateral governmental organizations for the purpose of protecting the vital interests of a data subject or other persons or to comply with laws governing reporting of communicable disease, including to assist such agencies or organizations in preventing exposure to or transmission of a communicable or quarantinable disease or to combat other significant public health threats; appropriate notice will be provided of any identified health threat or risk.

H. To hospitals, physicians, medical laboratories and testing facilities, and other medical service providers, for the purpose of diagnosing and treating medical conditions or arranging the care of patients who have been treated by DHS EMS providers.

I. To foreign governments for the purpose of coordinating and conducting the removal or return of aliens from the United States to other nations when disclosure of information about the alien's health is necessary or advisable to safeguard the public health, to facilitate transportation of the alien, to obtain travel documents for the alien, to ensure continuity of medical care for the alien, or is otherwise required by international agreement or law.

J. To immediate family members and attorneys or other agents acting on behalf of a patient to assist those individuals in determining the current medical condition and/or location of a patient to whom DHS has provided emergency medical care, provided they can present adequate verification of a familial or agency relationship with the patient.

K. To independent standardization and medical quality management

repositories, such as the National Emergency Medical Services Information System (NEMSIS), in de-identified, aggregate form only, to promote DHS compliance with emergency medical care industry standards and best practices.

L. To any person who is responsible for the care of the individual, to the extent necessary to assure payment of benefits to which the individual is entitled, when an individual to whom a record pertains is mentally incompetent or under other legal disability.

M. To the patient's health insurance company to facilitate any payment and billing negotiations between the patient, the insurance carrier and the agency.

DISCLOSURE TO CONSUMER REPORTING AGENCIES:

None.

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

STORAGE:

Records in this system are stored electronically or on paper in secure facilities in a locked drawer behind a locked door. The records are stored on magnetic disc, tape, digital media, and CD-ROM.

RETRIEVABILITY:

Records may be retrieved by any of the fields listed in the Categories of Records listed above.

SAFEGUARDS:

Records in this system are safeguarded in accordance with applicable rules and policies, including all applicable DHS automated systems security and access policies. Strict controls have been imposed to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions.

RETENTION AND DISPOSAL:

Based on the most conservative industry standards advised to implement Medical Quality Management, OHA will propose a retention schedule of ten (10) years from the date of the EMS provider encounter. Records will be retained pending the final approval by the National Archives and Records Administration of this records schedule.

SYSTEM MANAGER AND ADDRESS:

Director, Workforce Health and Medical Support Division, Office of

Health Affairs, Department of Homeland Security, Washington, DC 20528.

NOTIFICATION PROCEDURE:

Individuals seeking notification of and access to any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the Headquarters FOIA Officer, whose contact information can be found at <http://www.dhs.gov/foia> under "contacts." If an individual believes more than one component maintains Privacy Act records concerning him or her the individual may submit the request to the Chief Privacy Officer and Chief Freedom of Information Act Officer, Department of Homeland Security, 245 Murray Drive, SW., Building 410, STOP-0655, Washington, DC 20528.

When seeking records about yourself from this system of records or any other Departmental system of records your request must conform with the Privacy Act regulations set forth in 6 CFR part 5. You must first verify your identity, meaning that you must provide your full name, current address and date and place of birth. You must sign your request, and your signature must either be notarized or submitted under 28 U.S.C. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, you may obtain forms for this purpose from the Chief Privacy Officer and Chief Freedom of Information Act Officer, <http://www.dhs.gov> or 1-866-431-0486. In addition you should provide the following:

- An explanation of why you believe the Department would have information on you;
- Identify which component(s) of the Department you believe may have the information about you;
- Specify when you believe the records would have been created;
- Provide any other information that will help the FOIA staff determine which DHS component agency may have responsive records; and
- If your request is seeking records pertaining to another living individual, you must include a statement from that individual certifying his/her agreement for you to access his/her records.

Without this bulleted information the component(s) may not be able to conduct an effective search, and your request may be denied due to lack of specificity or lack of compliance with applicable regulations. Consistent with 6 CFR 5.22(f) *Release of Medical Records*, and pursuant to 5 U.S.C. 552a(f)(3), where requests are made for access to medical records, including

psychological records, the decision to release directly to the individual, or to withhold direct release, shall be made by a medical practitioner. Where the medical practitioner has ruled that direct release will cause harm to the individual who is requesting access, normal release through the individual's chosen medical practitioner will be recommended. Final review and decision on appeals of disapprovals of direct release will rest with the General Counsel.

RECORD ACCESS PROCEDURES:

See "Notification procedure" above.

CONTESTING RECORD PROCEDURES:

See "Notification procedure" above.

RECORD SOURCE CATEGORIES:

Records are obtained from DHS EMS medical care providers and their patients, either in the care and custody of the Department, at the DHS workplace, or in conjunction with a medical emergency where an on-duty DHS EMS is the medical care provider.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

Dated: August 23, 2011.

Mary Ellen Callahan,

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. 2011-22169 Filed 8-29-11; 8:45 am]

BILLING CODE 4410-9K-P

DEPARTMENT OF HOMELAND SECURITY

Coast Guard

[Docket No. USCG-2011-0821]

Merchant Mariner Medical Advisory Committee

AGENCY: Coast Guard, DHS.

ACTION: Notice of federal advisory committee meeting.

SUMMARY: The Merchant Mariner Medical Advisory Committee (MMMAC) will hold its inaugural meeting starting Monday, September 19, and ending Wednesday September 21, 2011. The meetings will be open to the public.

DATES: MMMAC will meet on Monday, September 19, Tuesday, September 20, and Wednesday, September 21, 2011 from 8:30 a.m. to 4:30 p.m. Please note that the meeting may close early if the committee has completed its business.

ADDRESSES: The meeting will be held at the Calhoun Marine Engineers Beneficial Association (MEBA) Engineering School at 27050 Saint Michaels Road, Easton, MD 21601.