## 1. Contact Information

**Department of State Privacy Coordinator**
Margaret P. Grafeld
Bureau of Administration
Information Sharing Services
Office of Information Programs and Services

## 2. System Information

(a) Date PIA was completed: May 18, 2010

(b) Name of system: Electronic Medical Record

(c) System acronym: eMED

(d) IT Asset Baseline (ITAB) number: 299

(e) System description

The Electronic Medical Record (eMED) system establishes the essential medical record infrastructure that the Department of State must have to provide quality health care services for all U.S. Foreign Affairs agencies worldwide. eMED establishes a single authoritative source of information that is readily retrievable for the following requirements: patient care, medical evacuations and hospitalizations, medical clearance decisions, medical record release actions, medical program planning and management, and immunization tracking. eMED provides a standardized and secure method to enter new medical record information into a patient's Department of State medical record, and to convert existing paper medical record data into electronic form.

(f) Reason for performing PIA:

☐ New system

**X Significant modification to an existing system**

☐ To update existing PIA for a triennial security reauthorization

(g) Explanation of modification:

MED is proposing to implement a significant change to the current eMED system that will alter the existing information flow. The proposed change involves implementing an inbound fax gateway to be housed in the HST Enterprise Server Operations Center (ESOC) in a DMZ environment, on a locally segregated network. The fax server will receive faxes sent from Foreign Service employees, Health Units, and consultants. These images will be stored temporarily, and then converted into TIFF images. An OpenNet server will connect to the fax server in the DMZ and securely download the images to be included in the eMED image system. Once the images are downloaded to OpenNet, the images on the fax server will be deleted.

(h) Date of previous PIA (if applicable): May 13, 2009

## 3. Characterization of the Information

The system:

☐ does NOT contain PII. If this is the case, you must only complete Section 13.

X does contain PII. If this is the case, you must complete the entire template.

### a. What elements of PII are collected and maintained by the system? What are the sources of the information?

Medical and demographic information (e.g., name, street address, SSN, DOB, email, phone number,) are collected for Department of State employees and eligible family members. Within the eMED system, each DoS employee/dependent is linked to their medical record through a unique ID number that is auto-generated during registration. The eMED system does not rely solely on the SSN for identification purposes (and does not collect SSN information for dependent records). The eMED system uses the SSN as a data point when registering an employee, so that duplicate records are not created. Once an employee and his/her family members are registered, each one has a unique Patient ID that is automatically generated by the system, which is then used as the primary identifier in eMED.

The information contained in eMED is obtained directly from the patients (Foreign Service employees and their eligible family members; civil service employees and their eligible family members working at overseas posts); from Health Unit and MED Exam Clinic clinicians; and from medical professionals consulted during a clearance or Medevac event.

### b. How is the information collected?

The information is collected from the patient through interviews and medical examinations conducted by the clinicians and medical professionals. Paper-based records, consisting of laboratory results from labs other than those affiliated with MED in the Washington, DC area, consults from specialists, and some administrative documents, are scanned into an electronic file that is associated with the patient's ID.

### c. Why is the information collected and maintained?

Name, social security number, and date of birth are used for verification of patients. Address and phone numbers are collected to contact the patient if required.

### d. How will the information be checked for accuracy?

MED verifies the accuracy of the demographic information for Foreign Service personnel and dependents against the Department of State HR database. It is the responsibility of the individual to ensure the accuracy of that information, and to submit corrections to the Human Resources division at the Department of State. For non-Foreign Service personnel, MED relies on oral and written information from patients.

For medical information, medical professionals perform periodic quality reviews to ensure that the information in the system is accurate.

### e. What specific legal authorities, arrangements, and/or agreements define the collection of information?

- 22 U.S.C. § 4084
- 42 U.S.C. § 290dd-1
- Pub. L. 99-570 §§ 7361-7362 and
- 5 C.F.R. Part 792

### f. Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

Confidentiality of patient medical information and PII poses a risk. MED mitigates the risk in these ways:

- Access to and printing of patient data and scanned images is fully audited.
- User access is role-based, and granted only at a supervisor's request.
- MED conducts annual HIPAA training to promote awareness of patient privacy rights.
- The data in eMed is only accessible on the DoS Intranet.

## 4. Uses of the Information

### a. Describe all uses of the information.

eMED provides a standard, rapid and secure way to enter information into a patient's medical record and enables patient's medical records to be available for use in one electronically secure and integrated file. The information retrieved is used to administer the appropriate health care services, and also for authentication and location purposes.

### b. What types of methods are used to analyze the data? What new information may be produced?

eMED has the capability to deliver multiple types of reports. The reports are used to examine trends in medical care delivery, medical condition, health awareness and epidemiology. Only DoS medical personnel have access to these reports based on the access controls guided by their business roles and permission. In case of emergency, the reports are provided to the proper authorities on a need-to-know basis in accordance with the HIPAA rule.

eMed does not in itself "analyze" data, but rather pulls raw data (whether patient-specific, such as their immunization report; or aggregate statistics, such as number of immunizations of a certain type provided over a certain period of time). The data could, however, be used to perform patient or patient community trend analysis.

### c. If the system uses commercial information, publicly available information, or information from other Federal agency databases, explain how it is used.

Not applicable.

### d. Are contractors involved in the uses of the PII?

Contractors are involved with the design, development, and maintenance of the system. Each contract contains a Privacy Act clause informing the contractors of their responsibilities regarding privacy. Annual training is provided to all users and non-users of the system regarding the handling of sensitive information and information processing systems.

### e. Privacy Impact Analysis: Describe the types of controls that may be in place to ensure that information is handled in accordance with the above uses.

Medical professional standards indicate that any unauthorized use and monitoring of medical information for reasons other than primary care is unacceptable. Access to the system and data is determined by each individual's business need and role. The access rules have been identified in the eMED's user requirements documentation. Prior to accessing the eMED system, each user must read and agree to a disclaimer regarding accessing and reviewing patient medical information.

## 5. Retention

### a. How long is information retained?

For employees who have separated from the Federal Government, their paper records are retired to National Personnel Record Center (NPRC) in St. Louis, Missouri one year after separation. NPRC will destroy the records 75 years after the birth date of the employee, 60 years after the date of the earliest document in the folder if the birth cannot be ascertained, or 30 years after the latest separation, whichever is later.

MED is developing a policy and method for archiving electronic medical records, which we have been accumulating for about 8 years.

### b. Privacy Impact Analysis: Discuss the risks associated with the duration that data is retained and how those risks are mitigated.

Lack of accessibility is a risk posed by record retention policies for electronic records. Our methods must include a process for rapid record retrieval. In addition, MED must be mindful that any transition to new EMR systems should include migration of "active" data.

## 6. Internal Sharing and Disclosure

### a. With which internal organizations is the information shared? What information is shared? For what purpose is the information shared?

Internal organizations with whom information is shared include the originating office (MED) and the Bureau of Human Resources (HR). Information pertaining to physical examination date, medical clearance determination and medical clearance date is shared.

### b. How is the information transmitted or disclosed? What safeguards are in place for each sharing arrangement?

The information is transmitted from eMED into HR via an interface between eMED and HR's Foreign Service Assignment Management Application. Information/data is available only to authorized users of the application. Authorized users have roles assigned to them specific to their job function. Thus, a strong segregation of duties is in place.

### c. Privacy Impact Analysis: Describe risks to privacy from internal sharing and disclosure and describe how the risks are mitigated.

Internal sharing occurs only with authorized users who are cleared U.S. government employees or contractors with work-related responsibility, specific to the access and use of the system's data. No other internal disclosures of the information/data within the Department are made.

## 7. External Sharing and Disclosure

### a. With which external organizations is the information shared? What information is shared? For what purpose is the information shared?

The following are examples of permitted uses and disclosures of an individual's protected health information:

- Health information is disclosed to the Secretary of the Department of Health and Human Services for investigations or determinations of compliance with laws on the protection of health information.
- To provide, coordinate, or manage your health care and any related service, as necessary for provision of any diagnosis and prescriptions/medications in a DoS health unit/clinic.
- For consultation by another physician or health care provider (for example, a specialist, pharmacist, or laboratory) who, at the request of an individual's physician, becomes involved in your care by providing assistance with your health care diagnosis or treatment. This includes pharmacists who may need to provide information on other drugs an individual has been prescribed to identify potential interactions.
- In emergencies to provide the required treatment.
- To obtain payment for health care services, including services recommended for determining eligibility for benefits, and utilization reviews.
- To support the daily activities related to health care which may include, but are not limited to, quality assessment activities, investigations of adverse events or complaints, medical suitability determinations for medical and security clearances, medical clearance of an individual for a specific post, oversight of staff performance, and conducting or arranging for other health care related activities.
- To a health oversight agency for activities such as audits, investigations, and inspections. These health oversight agencies might include government agencies that oversee the health care system, government benefit programs, other government regulatory programs, and civil rights laws.

- For use in a judicial or administrative proceeding, in response to a court order or administrative tribunal and in certain conditions in response to a subpoena, discovery request, or other lawful process.
- Information requests for identification and location of individuals.
- Circumstances pertaining to victims of a crime.
- Deaths suspected from criminal conduct.
- Crimes occurring at a Department of State facility.
- Medical emergencies (not on the DoS premises) believed to result from criminal conduct.
- To prevent or lessen a serious and imminent threat to the health or safety of another person or the public.
- To a public health authority who is permitted by law to collect or receive the information. The disclosure may be necessary to do the following:
    - Prevent or control disease, injury, or disability;
    - Report births and deaths;
    - Report reactions to medications or problems with products;
    - Notify a person who may have been exposed to a disease or may be at risk for contracting or spreading a disease or condition;
    - Notify the appropriate government authority if we believe a patient has been the victim of abuse, neglect, or domestic violence and
    - To a person who might have been exposed to a communicable disease or might otherwise be at risk of contracting or spreading the disease or condition.
- To a person or company required by the Food and Drug Administration (FDA) to do the following:
    - Report adverse events, product defects, or problems and biologic product deviations;
    - Track products;
    - Enable product recalls;
    - Make repairs or replacements; and
    - Conduct post-marketing surveillance as required.
- To coroners or medical examiners for identification, to determine the cause of death, or for the performance of other duties authorized by law. Protected health information may also be disclosed to funeral directors as authorized by law.
- To authorized Federal officials for conducting national security and intelligence activities and protective services to the President or others.

### b. How is the information shared outside the Department? What safeguards are in place for each sharing arrangement?

MED complies with legal requirements in the Health Insurance Portability and Accountability Act (HIPAA) regulations and elsewhere for reporting healthcare related events. To comply with HIPAA requirements, MED provides the information in paper format only, and a receipt for change of custody is maintained for information that is shared. An audit trail is also

recorded in eMED for all documents printed, including the reasons for printing as well as the recipient.

### c. Privacy Impact Analysis: Describe risks to privacy from external sharing and disclosure and describe how the risks are mitigated.

External sharing occurs only with authorized users who are cleared U.S. Government employees or contractors with work-related responsibility, specific to the access and use of the system's data. These external disclosures are in compliance with the law.

## 8. Notice

The system:

X contains information covered by the Privacy Act.

**State-24, Medical Record**

☐ does NOT contain information covered by the Privacy Act.

### a. Is notice provided to the individual prior to collection of their information?

In accordance with the Privacy Act and HIPAA, a patient is made aware of the possible uses and disclosure of their health information, and asked to sign acknowledgement of this notice.

### b. Do individuals have the opportunity and/or right to decline to provide information?

Individuals can decline to provide a signed acknowledgment and provide information. Failure to disclose medical information needed from you by Medical Services may affect their ability to provide treatment or (in the case of medical clearances) may result in denial of a medical clearance.

### c. Do individuals have the right to consent to limited, special, and/or specific uses of the information? If so, how does the individual exercise the right?

An individual can request that Medical Services not use or disclose any part of his/her protected health information. The request must be made in writing to the Medical Services Privacy Officer where the individual wishes the restriction instituted. The request must include (1) information to be restricted; (2) whether a restriction applies to Medical Services use, disclosure, or both; (3) to whom the restriction applies (for example, disclosures to a spouse); and (4) an expiration date. Medical Services is not required to agree to a requested restriction. If the restriction is mutually agreed upon, the individual's request will be honored, unless it is needed to provide emergency treatment. The individual may revoke a previously agreed-upon restriction, at any time, in writing. All disclosure restrictions expire in five years and must be renewed if the individual wants them continued.

### d. Privacy Impact Analysis: Describe how notice is provided to individuals and how the risks associated with individuals being unaware of the collection are mitigated.

Medical records are privileged and controlled by Privacy Act, HIPAA and other legislation/regulation. The policy on use and disclosure of medical records is given to every patient and is also available on the Office of Medical Services website.

## 9. Notification and Redress

### a. What are the procedures to allow individuals to gain access to their information and to amend information they believe to be incorrect?

If you believe that the information maintained in eMED is incorrect or incomplete, you may request an amendment to your information. If there are factual errors (wrong birth date, wrong blood type, etc.), this information will be corrected. If you disagree with statements in the record, the statement will be amended, but the original document cannot be changed. You may submit a written request for amendment to the Medical Privacy Officer, U.S. Department of State; The Office of Medical Services M/MED/QI; SA-1; Washington D.C. 20522-0102.

### b. Privacy Impact Analysis: Discuss the privacy risks associated with notification and redress and how those risks are mitigated.

The risk associated with Notification and Redress is mitigated by the aforementioned SORN (Medical Records, STATE-24).

## 10. Controls on Access

### a. What procedures are in place to determine which users may access the system and the extent of their access? What monitoring, recording, and auditing safeguards are in place to prevent misuse of data?

The use of any eMED components by Department MED personnel is dependent upon access control, as determined by supervisors. Access control authorizes individual, module-specific access rights upon valid user authentication. The eMED login process is a two-tiered process. The login validates a user's security identifier (user name) and access rights/roles permissions within the eMED system. Within each module of eMED each user has a specific role and permissions that apply to the function of that role within the eMED database. When a user logs on, the user name and password are checked against the username within the Oracle database. If the username correlates to one on file, application-specific access rights are granted to the user. The eMed database forces a password change every 180 days.

Access to and printing of patient data and scanned images is fully audited.

### b. What privacy orientation or training for the system is provided authorized users?

All users are required to undergo computer security and privacy awareness training prior to accessing the system, and must complete refresher training yearly in order to retain access. MED also has developed HIPAA training, which all MED users are required to take.

### c. Privacy Impact Analysis: Given the sensitivity of PII in the system, manner of use, and established access safeguards, describe the expected residual risk related to access.

Residual risk related to access is the consequence of the inconsistent or overlooked implementation of the several controls described in this Section.

## 11. Technologies

### a. What technologies are used in the system that involve privacy risk?

There are no technologies in place to elevate the privacy risk of the system data. The data is stored in an Oracle database and is not shared with other applications. The database resides in a secure environment located behind a managed firewall. There are no external connections to this environment. Flaw remediation software such as antivirus protection and encryption technology is in place. In addition, all authorized users are required to login and be authenticated at the network level before access to the system data is granted.

### b. Privacy Impact Analysis: Describe how any technologies used may cause privacy risk, and describe the safeguards implemented to mitigate the risk.

No such risk is anticipated.

## 12. Security

### What is the security certification and accreditation (C&A) status of the system?

eMED was certified and accredited on November 2007. The authorization is valid for 36 months. The C&A certification will expire on November 30, 2010.