

## 1. Contact Information

**Department of State Privacy Coordinator**

Margaret P. Grafeld  
Bureau of Administration  
Global Information Services  
Office of Information Programs and Services

## 2. System Information

- (a) Date PIA was completed: May 6, 2009
- (b) Name of system: Electronic Medical Record
- (c) System acronym: eMED
- (d) IT Asset Baseline (ITAB) number: 299
- (e) System description (Briefly describe scope, purpose, and major functions):

Electronic Medical Record (eMED) is a series of integrated systems which replaces paper-based medical examination/evaluation forms and letters and archives past paper records in an image file format. The eMED System establishes the essential medical record infrastructure that the Department of State (DoS) must have to provide quality health care services for all U.S. Foreign Affairs agencies worldwide. The eMED establishes a single authoritative source of information that is readily retrievable for: patient care, medical evacuations and hospitalizations, medical clearance decisions, medical record release actions, medical program planning and management, and immunization tracking. The eMED converts existing paper medical record data to electronic data. It provides a standard, rapid and secure way to enter new medical record information into a patient's DoS medical record. Medical records on a patient, which are fragmented on paper in many geographically disparate locations, will be available for use in one secure and integrated medical record electronically. The eMED has the ability to generate a complete record of a clinical patient encounter.

- (f) Reason for performing PIA:
  - New system
  - Significant modification to an existing system
  - To update existing PIA for a triennial security re-certification

(g) Explanation of modification (if applicable):

(h) Date of previous PIA (if applicable): July 2008

## 3. Characterization of the Information

The system:

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

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?**

The system collects the following:

- Name;
- Social security number;
- Date of birth;
- Street address to include email and
- Phone number

The sources of the information are Foreign Service employees, eligible family members and Civil Service employees working at posts abroad.

**b. How is the information collected?**

The information is collected from the patient through interview and medical examination. Paper-based records are converted to electronic medical record.

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

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

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

It is the responsibility of the individual to ensure the accuracy of the information collected during the interview process. Medical professionals also perform 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.**

The privacy risks are low. The minimum amount of personally identifiable information is collected to satisfy the purpose of this system.

**4. Uses of the Information**

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

It provides a standard, rapid and secure way to enter information into a patient's medical record thereby enabling a patient's medical records to be available for use in one electronically secure and integrated file.

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

The eMED has the capability to deliver multiple reports. The reports will be used to examine trends in medical care delivery, medical condition, health awareness and epidemiology. Only Department medical personnel will have access to these reports based on the access control guided by their business roles and permission. In case of emergency, the reports are provided to the proper authority on a "need to know" basis following the Health Insurance Portability and Accountability Act (HIPAA) rule.

**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. Is the system a contractor used and owned system?**

Contractors are involved with the design and development 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 eMed 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 state that any unauthorized use and monitoring of medical information for reasons other than primary care is unacceptable. Access to the system and data are determined by each individual's business need and role. The access rules have been identified in the eMED's User Requirements documentation.

## **5. Retention**

**a. How long is information retained?**

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

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

Access to computerized files is password-protected and under the direct supervision of the system manager. When records have reached their retention period, they are immediately retired or destroyed in accordance with the National Archive and Records Administration (NARA) disposition schedules.

## **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 which the information is shared include the originating office and the Bureau of Human Resources (HR). Information pertaining to the physical examination date, medical clearance determination and medical clearance date is shared. The information is shared for medical clearance related to employment.

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

The information is transmitted from eMED into the Bureau of Human Resources (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, 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 of State 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?**

Following are examples of permitted uses and disclosures of your protected health information:

- Health information is disclosed to the Secretary of the Department of Health and Human Services (HHS) 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 Department of State health unit/clinic.
- To another physician, or health care provider (for example, a specialist, pharmacist, or laboratory) who, at the request of your physician, becomes involved in your care by providing assistance with your health care diagnosis or treatment. This includes pharmacists who may be provided information on other drugs you have been prescribed to identify potential interactions.
- In emergencies to provide the required treatment.
- To obtain payment for your 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.
- 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 Department of State 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 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. We may also disclose protected health information 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?**

The Office of Medical Affairs (M/MED) complies with legal requirements in the HIPAA regulations and elsewhere for reporting healthcare related events. To comply with HIPAA requirements, M/MED will provide 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, 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:

- constitutes a system of records covered by the Privacy Act. State-24, Medical Record
- does not constitute a system of records covered by the Privacy Act System

**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 M/MED may affect their ability to provide treatment or (in the case of medical clearances) may result in denial of 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?**

Individual can request that M/MED not use or disclose any part of his/her protected health information. Request must be made in writing to the Medical Service Privacy Officer where the individual wishes the restriction instituted. The request must include: (1) the information to be restricted; (2) whether a restriction applies to M/MED use, disclosure, or both; (3) to whom the restriction applies to, for example, disclosures to a spouse; and (4) an expiration date. M/MED 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.**

Individuals' medical records are privileged and controlled by the Privacy Act, HIPAA and other legislation/regulations. The policy on the 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 information maintained in eMED is incorrect or incomplete, you may request an amendment to your information. If there are factual errors (incorrect birth date, incorrect 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 DC 20522-0102.

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

There is no risk associated with Notification and Redress as it is a part of the system of records notice: 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 usages of all eMED components used by DoS medical providers are dependent upon access control. Access control authorizes individual module specific access rights and 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. Users are forced to change passwords every 180 days by system administrators. Users are not allowed to manually change passwords without the prompting of a system administrator.

- 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.

- 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.**

No such residual risk anticipated.

## **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?**

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