Department of State
Privacy Impact Assessment
Electronic Medical Record System
Updated July 2008

A. CONTACT INFORMATION:

Who is the Agency Privacy Coordinator who is conducting this assessment? (Name, organization, and contact information).

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

B. SYSTEM APPLICATION/GENERAL INFORMATION:

1) Does this system contain any personal information about individuals or *personally identifiable information? If answer is no, please reply via e-mail to the following e-mail address: pia@state.gov. If answer is yes, please complete the survey in its entirety.

YES __X__ NO___

2) What is the purpose of the system/application?

The Electronic Medical Record (EMR) System establishes the essential medical record infrastructure to provide quality health care services for all U.S. Foreign Affairs agencies worldwide. The EMR system 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 EMR System converts the data on existing paper medical records to electronic data and provides a standard, rapid and secure way to enter new medical record information into a patient's Department medical record. With the EMR System, medical records on a patient will be available for use in one electronically secure and integrated file.

3) What legal authority authorizes the purchase or development of this system/application?

Legal authority to procure a design and development of an electronic record system is derived from the Government Paperwork Elimination Act (GPEA), the Paperwork Reduction Act (PRA), and the e-Government Act of 2002.

C. DATA IN THE SYSTEM:

1) Does a Privacy Act system of records description already exist?

YES _X__ NO_ __

If yes, please provide the following:
System Name: Medical Records

2) What categories of individuals are covered in the system?

Individuals covered in the EMR System are Foreign Service employees, eligible family members (EFMs) and Civil Service employees working at overseas posts.

3) What are the sources of the information in the system?

a. Is the source of the information from the individual or is it taken from another source? If not directly from the individual, then what other source?

The information contained in the EMR is taken from the individual. The medical information contained in the EMR system is derived via interview sessions and medical examinations of each patient.

b. Why is the information not being obtained directly from the individual?

Not applicable.

c. What Federal agencies are providing data for use in the system?

Not applicable.

d. What State and/or local agencies are providing data for use in the system?

Not applicable.

e. From what other third party sources will data be collected?

Individuals have the option of having a third party physician completing their information. As such, the medical information obtained from the third party physician is contained in the EMR.

f. What information will be collected from a State Department employee and the public?

Medical and demographic information is collected from Department employees and eligible family member(s) (EFM).

3) **Accuracy, Timeliness, and Reliability**

a. **How will data collected from sources other than DOS records be verified for accuracy?**

MED medical professionals adhere to professional medical protocols. These protocols include quality review to ensure that the information in the system is accurate. Information that is collected from other sources is processed through the medical records scan and review process that includes performing quality checks of the scanned records for accuracy, and performing final quality review by each medical professional who views the information.

b. **How will data be checked for completeness?**

Quality checks for accuracy, and final quality reviews by each medical professional who views the information.

c. **Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date? Name the document (e.g., data models).**

The data in the system is current as of the last interaction/communication with the individual.

d. **Are the data elements described in detail and documented? If yes, what is the name of the document?**

The data elements are described in detail and documented both in the system and in the system requirements document.

D. <u>DATA CHARACTERISTICS:</u>

1) **Is the use of the data both relevant and necessary to the purpose for which the system is being designed?**

Yes.

2) **Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed?**

The system can derive new data or create previously unavailable data about an individual through aggregation via the reporting mechanism. These reports are maintained separately in the system database.

3) **Will the new data be placed in the individual's record?**

Yes.

4) **Can the system make determinations about employees/public that would not be possible without the new data?**

No.

5) **How will the new data be verified for relevance and accuracy?**

Quality checks for accuracy, and final quality reviews by each medical professional who views the information.

6) **If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?**

Usage of all EMR components by Department medical personnel is dependent upon access control. Access control authorizes each individual specific access rights and valid user authentication. The EMR login process is a two-tiered process. First the login validates a user's security identifier (user name), then the user's access rights/roles permissions. 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 database. If the username correlates to one on file, application specific access rights are granted. Users are prompted to change passwords every 180 days, but are not allowed to manually change passwords without the prompting of a system administrator.

7) **If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access?** Explain.

See answer above.

8) **How will the data be retrieved? Does a personal identifier retrieve the data? If yes, explain and list the identifiers that will be used to retrieve information on the individual.**

Data may be retrieved from the EMR system using the patient's name, social security number, date of birth and patient ID.

9) What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?

EMR 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 Department of State medical personnel have access to these reports based on the access control guided by their business roles.

In case of an emergency, the reports are provided to the proper authority on a "need to know" basis per HIPAA guidelines.

E. MAINTENANCE AND ADMINISTRATIVE CONTROLS:

1) If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?

Not applicable.

2) What are the retention periods of data in this system?

The retention period for active employees and eligible family members is through the duration of the individual's employment or eligibility of a family member under the medical program.

3) What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?

When required, data will be disposed of as an individual record, with the disposition instructions taking effect once the employee has transferred or separated. Employees' records will be retired to NPRC St. Louis, Mo., one year after separation. NPRC will destroy the records 75 years after 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.

4) Is the system using technologies in ways that the DOS has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?

No.

5) How does the use of this technology affect public/employee privacy?

Not applicable.

6) Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.

Yes. The system will be able to identify individuals and their medical information; locate them based on their most recent physical, which indicates the overseas post to which they are assigned; and monitors any change in their medical condition.

7) What kinds of information are collected as a function of the monitoring of individuals?

For monitoring purposes, the only information collected and reported are items related to a change(s) in an individual's medical condition.

8) What controls will be used to prevent unauthorized monitoring?

Medical professional standards indicate that any unauthorized use and monitoring of medical information for reasons other than primary care is unacceptable. Access to the EMR System and any monitoring is strictly based on the specific business role of any user given access to the system.

10) If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.

The system is not being modified.

11) Are there forms associated with the system? YES __X__ NO ___
If yes, do the forms include Privacy Act statements that include required information (e.g. – legal authorities allowing for the collection of the information being requested, whether provision of the information is mandatory or voluntary, the routine uses of the data, with whom the data will be shared, the effects on the individual if the data is not provided)?

Each form does contain a Privacy Act statement that includes the required information identified by the Privacy Act regulation.

F. ACCESS TO DATA:

1) Who will have access to the data in the system? (e.g., contractors, users, managers, system administrators, developers, other)

Contractors, direct hire medical personnel, and system administrators.

2) How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?

Access to the system and data are determined by each individual's business "need to know" and business role. The access rules are stated in the EMR User Requirements documentation.

3) **Will users have access to all data on the system or will the user's access be restricted? Explain.**

   User access is determined by specific user role and need-to-know. If an individual's role does not require access to the system, he/she will be restricted from accessing the system.

4) **What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access? (Please list processes and training materials.)**

   The system is configured with full access auditing at the database level. The auditing records all events including what data was accessed and/or modified. In the event of a modification – the original data before the modification is recorded, then the date and time when a modification was effected and by whom.

5) **Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed? Have rules of conduct been established and training regarding the handling of such information under the Privacy Act of 1974, as amended?**

   Contractors are involved with the design and development of the system. Each contract contains Privacy Act clauses informing the contractors of their responsibilities regarding privacy. Annual training is provided to all users and non-users of the system (as part of their security training) regarding the handling of sensitive information and information processing systems.

6) **Do other systems share data or have access to the data in the system? If yes, explain.**

   Yes. A human resource interface exists between EMR and the Bureau of Human Resources (HR). Data is transmitted from EMR into an HR access database. The type of data being transmitted includes an individual's last name, first name, middle initial, social security number, date of birth, registration date, external physical examination date, medical clearance determination, and the medical clearance date.

7) **Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?**

The Privacy Officer in the Office of Medical Services (MED).

8) Will other agencies share data or have access to the data in this system (Federal, State, Local, Other)?

No.

9) If so, how will the data be used by the other agency?

No.

10) Who is responsible for assuring proper use of the data?

Office of Medical Services Privacy Officer and Office of Medical Services, ISSO.