Submit the completed PIA to
Privacy's SharePoint Customer Center

eMed v02.02

1. Contact Information

A/GIS Deputy Assistant Secretary
Bureau of Administration
Global Information Services

2. System Information

(a) Name of system: eMed v02.02

(b) Bureau: Bureau of Medical Services

(c) System acronym: eMed

(d) iMatrix Asset ID Number: 299

(e) Reason for performing PIA: Click here to enter text.

- ☐ New system
- ☐ Significant modification to an existing system
- ☒ To update existing PIA for a triennial security reauthorization

(f) Explanation of modification (if applicable): Click here to enter text.

3. General Information

(a) Does the system have a completed and submitted Security Categorization Form (SCF)?

☒Yes

☐No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

(b) What is the security Assessment and Authorization (A&A) status of the system?

ATO expires 9/30/2017. Re-authorization process to begin soon.

(c) Describe the purpose of the system:

The Electronic Medical Record (eMED) system establishes the essential medical record infrastructure that allows the Department of State 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.

(d) Describe the personally identifiable information (PII) that the system collects, uses, maintains, or disseminates:

Medical and demographic information is collected for Department of State, other agency employees and eligible family members. Information that is required for all registrants includes:

- Last Name
- First Name
- Date of birth
- Gender
- For Foreign Service employees only, a Social Security number is required.

"Family units" are created during the registration of the employee, and information entered for each family member includes "relationship to employee," and employee's agency. Other PII that is not required but may be collected includes middle initial, suffix, current post, place of birth; temporary and permanent street addresses, telephone numbers, and email addresses; and emergency contact information (address, phone number, and email address). Within the eMED system, each DoS employee/dependent is linked to his/her 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 dependents or non-State records). The eMED system uses the SSN as a data point when registering an employee, so that duplicate records are not created. The use of SSN is a requirement based on the registration data that HR feeds eMED. MED verifies the accuracy of the demographic information for Foreign Service personnel and dependents against the Department of State HR database. 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.

eMed is a medical record of patient visits to MED's exam clinic or submission of examination information to Medical Clearances for purposes of being medically cleared for assignment to overseas duty. eMed also contains immunization information, lab test information, Medevac information, and consultations from various specialists.

(e) What are the specific legal authorities and/or agreements that allow the information to be collected?

- 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) Is the information searchable by a personal identifier (e.g., name or Social Security number)?
☒Yes, provide:
- SORN Name and Number: Medical Records, State-24
- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN): May 26, 2009

☐No, explain how the information is retrieved without a personal identifier.
Click here to enter text.

(g) Does the existing SORN need to be amended to reflect the inclusion of this new or significantly modified system? ☒Yes ☐No

If yes, please notify the Privacy Division at Privacy@state.gov.

(h) Is there a records retention schedule submitted to or approved by the National Archives and Records Administration (NARA) for this system? ☒Yes ☐No
(If uncertain about this question, please contact the Department's Records Officer at records@state.gov .)

If yes provide:
- Schedule number (e.g., (XX-587-XX-XXX)): A-12-001-01a
- Length of time the information is retained in the system: Currently no records in eMed have been destroyed or archived. An internal committee is working with the DoS Records Officer to define a clear and consistent schedule.
- Type of information retained in the system:
Medical records

4. Characterization of the Information

(a) What entities below are the original sources of the information in the system? Please check all that apply.
☐ Members of the Public
☒ U.S. Government employees/Contractor employees
☐ Other (people who are not U.S. Citizens or LPRs)

(b) If the system contains Social Security Numbers (SSNs), is the collection necessary?
☒Yes ☐No

- If yes, under what authorization?
The eMED system uses the SSN as a data point when registering an employee, so that duplicate records are not created. The use of SSN is a requirement based on the registration data that HR feeds eMED. MED verifies the accuracy of the demographic information for Foreign Service personnel and dependents against the Department of

State HR database. 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.

(c) How is the information collected?

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. The information is collected from the patient through interviews and medical examinations conducted by the clinicians and medical professionals. The information is also collected from Department forms DS1843 (Medical History and Examination for Foreign Service, for Individuals Age 12 and Older), DS1622 (Medical History and Examination for Foreign Service, for Individuals under Age 12), DS-3057 (Medical Clearance Update), or DS-6561 (Non-Foreign Service Personnel and their Family Members physical exam form), and scanned into an electronic file. Other paper-based records, consisting of external laboratory results, consults from specialists, and some administrative documents, are scanned into an electronic file that is associated with the patient's ID.

(d) Where is the information housed?

☒ Department-owned equipment

☐ FEDRAMP-certified cloud

☐ Other Federal agency equipment or cloud

☐ Other

- If you did not select "Department-owned equipment," please specify.

Click here to enter text.

(e) What process is used to determine if the information is accurate?

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 DoS/HR. 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.

(f) Is the information current? If so, what steps or procedures are taken to ensure it remains current?

Demographic and contact information for active patients is checked each time they submit clearance update information, are medevac'ed, or have a clinic appointment. For State Department employees and eligible family members (EFMs), this information can also be validated against the source information in the HR database.

(g) Does the system use information from commercial sources? Is the information publicly available?
No

(h) Is notice provided to the individual prior to the collection of his or her information?
Yes. A patient is made aware of the possible uses and disclosure of his or her health information on the DS-1843, DS-1622, DS-3057 or DS-6165, and asked to sign acknowledgement of this notice on the same form. Additionally, the system of records notice (SORN) listed above, State-24, provides notice to individuals of this type of information collection.

(i) Do individuals have the opportunity to decline to provide the information or to consent to particular uses of the information? ☒Yes ☐No

- If yes, how do individuals grant consent?

A patient is made aware of the possible uses and disclosure of his or her health information on the DS-1843, DS-1622, DS-3057 or DS-6165, and asked to sign acknowledgement of this notice on the same form.
Individuals can decline to provide a signed acknowledgment and provide information. Failure to disclose medical information needed from patients 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.

- If no, why are individuals not allowed to provide consent?
Click here to enter text.

(j) How did privacy concerns influence the determination of what information would be collected by the system?
The eMed system was redesigned in 2006, and at that time, we consciously removed any PII that was not necessary, and minimized the number of screens that display some information, such as SSN, as much as possible. We also stopped collecting SSN for any patients except Foreign Service employees (and Civil Service who need a medical clearance for a TDY).

5. Use of information

(a) What is/are the intended use(s) for the information?

eMED provides a standard, rapid and secure way to enter information into a patient's medical record and enables a patient's medical records to be available for use in one electronically secure and integrated file. The information retrieved is used for medical clearance determinations, Medevac research and documentation, immunization documentation, and delivery of healthcare services. The MED Clearance Dashboard tool provides real-time information to the patient regarding their medical clearance status.

Medical clearance determinations are made based on a patient's health information, as entered into eMed's clinical modules (if the patient was seen in MED's exam clinic) or as documented by submissions of externally-performed labs, consults, and exams.

The Medevac module of eMed is used to enter administrative and diagnostic information about a patient's medevac. The system enables better tracking of medevacuees' status and progress, and assists in making a clearance decision prior to their return to post.

Records are kept of all immunizations administered by MED's Washington, DC, health units, and externally-administered immunizations are also entered to build a complete record for the benefit of the patient and for the information of any MED practitioner with a need to know.

The eMED system uses the SSN as a data point when registering an employee, so that duplicate records are not created. The use of SSN is a requirement based on the registration data that HR feeds eMED. MED verifies the accuracy of the demographic information for Foreign Service personnel and dependents against the Department of State HR database. 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.

(b) Is the use of the information relevant to the purpose for which the system was designed or for which it is being designed?
Yes.

(c) Does the system analyze the information stored in it? ☐Yes ☒No*

* 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 raw data can be pulled from the database (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.

If yes:

(1) What types of methods are used to analyze the information?
Analysis is not done. Simple queries are run for reports.

(2) Does the analysis result in new information?
No.

(3) Will the new information be placed in the individual's record? ☐Yes ☒No

(4) With the new information, will the Department be able to make new determinations about the individual that would not have been possible without it?
☐Yes ☒No

6. Sharing of Information

(a) With whom will the information be shared internally and/or externally? Please identify the recipients of the information.
Internal organizations with which information from eMed is shared include the originating office (MED) and Human Resources (HR).
Information is not shared externally.

(b) What information will be shared?

When a medical clearance "class" has been electronically approved in eMed, that class "code" (a number between 1 and 9) is sent electronically, along with the date that the clearance was approved, to an HR database. The clearance information does not include any medical information. The personally identifiable information transmitted to HR is the same information that was previously downloaded from HR when registering the patient. That is, no new PII is conveyed back to HR. The transmitted information is sent in order to uniquely identify the patient, and includes last name, first name, MI, DOB, and employee's SSN.

(c) What is the purpose for sharing the information?
The information is shared with HR so that they know that a candidate/employee is medically cleared for assignment to post. A candidate's employment cannot be finalized without this information. An employee cannot travel to a new Post without this information.

(d) The information to be shared is transmitted or disclosed by what methods?
There is a direct database link between the eMed database and the HR database. eMed automatically communicates any new data up to HR every 20 minutes.

(e) What safeguards are in place for each internal or external sharing arrangement?

Information/data is available only to authorized MED and HR users of the respective applications. Authorized users have roles assigned to them specific to their job function and have limited access to information based on this role. For example, HR personnel do not have access to personal health information. Thus, a strong segregation of duties is in place.

(f) What privacy concerns were identified regarding the sharing of the information? How were these concerns addressed?

MED and HR are conscious of the need to balance patient privacy concerns with their need to have accurate and rapid communication of key data between our two groups. We have a long-standing MOU with HR that describes the specific data to be shared, and the method of sharing.

7. Redress and Notification

(a) What procedures allow individuals to gain access to their information?

Individuals can submit written requests to our Medical Records department for copies of the information in their eMed record. Individuals may only request for themselves or minor children.

(b) Are procedures in place to allow an individual to correct inaccurate or erroneous information?

☒Yes ☐No

If yes, explain the procedures.

An individual can inform Medical Records (MR) of the presence of inaccurate information. Depending on the nature of the inaccuracy, Medical Records will make the correction, request further information from the individual, refer the request to Medical Informatics (if a change cannot be made from the application front end), or refer the request to MED Management for review.

If no, explain why not.

Click here to enter text.

(c) By what means are individuals notified of the procedures to correct their information?

Individuals would communicate with Medical Records via email or phone contact. MR also has information posted on their Sharepoint site for contacting them.
http://med.m.state.sbu/ex/mi/records/default.aspx

8. Security Controls

(a) How is the information in the system secured?

The data is contained in an Oracle database that is secured to Department standards, including encryption of data at rest. Access controls built into the system limit users to

only those aspects of eMed required to perform their job. Direct database access is limited to two MED IT individuals who have database positions/skills.

(b) Describe the procedures established to limit access to only those individuals who have an "official" need to access the information in their work capacity.

The use of any eMED components by DoS MED clinical 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 60 days.

(c) What monitoring, recording, and auditing safeguards are in place to prevent the misuse of the information?

Every aspect of user activity within the eMed system is audited; audit records are kept within the Oracle database, and can easily be queried as needed.

Any part of a record printed from eMed carries a watermarked serial number that is also recorded in the database.

(d) Explain the privacy training provided to authorized users of the system.

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.

All Department of State Foreign Service (FS) and Civil Service (CS) employees are required to pass the PA459, Protecting Personally Identifiable Information (PII), course. Locally Employed (LE) Staff who handle PII are also required to take the course.

New eMed users sign a "Rules of Behavior," indicating that they understand the rules they must follow to be allowed access to the system.

(e) Are any security controls, such as encryption, strong authentication procedures, or other controls, in place to make the information unusable to unauthorized users? ☒Yes ☐No

If yes, please explain.

The data is encrypted at rest and in transit.

The eMed system employs single sign-on, comparing the Opennet user ID of the user who is logged on to the workstation and who launches eMed against the Oracle records of users who have valid eMed accounts. Further, all workstations in MED require the use of a PIV card to log on.

(f) How were the security measures above influenced by the type of information collected?
eMed's security categorization is "Moderate" because of the PII it contains. All measures required by NIST to secure a Moderate-level application has been taken and are continuously monitored.

9. Data Access

(a) Who has access to data in the system?
Only employees of MED have access to the eMed system. These employees include both direct-hire and contract-hire doctors, nurses, psychologists, social workers, lab technicians, clerks, and system administrators. Overseas, access to eMed data is limited to direct-hire clinicians and to cleared, locally employed staff and clinical health unit staff. While all employees with access are formally cleared, the level of security clearance required for their position and their access to eMed is determined by the business unit supervisor and/or the contract.

(b) How is access to data in the system determined?
The use of any eMED components by DoS MED clinical personnel is dependent upon access control, as determined by supervisors. Access control authorizes individual, module-specific access rights upon valid user authentication.

In order to support customers, eMed system administrators have access to all system modules via eMed administrator accounts. In order to provide Tier 3 support, MED's database administrators also have elevated privileges and the necessary tools to access eMed's Oracle database directly.

(c) Are procedures, controls or responsibilities regarding access to data in the system documented? ☒Yes ☐No

(d) Will all users have access to all data in the system, or will user access be restricted? Please explain.
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.

(e) What controls are in place to prevent the misuse (e.g. unauthorized browsing) of data by users having access to the data?

Every action in eMed, including browsing of a record, is audited in the database. Though there are no specific patient records in eMed that are blocked from viewing by authenticated users, there are pieces of information, such as mental health records, that are restricted to use by very limited groups of users. If any concern were to be raised about unauthorized browsing, eMed database administrators can look at audit records on either a per user, per patient, or per screen basis.