# PRIVACY IMPACT ASSESSMENT

## eMED 02.06.00

### 1. Contact Information

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

### 2. System Information

**(a) Date of completion of this PIA:** July 2022
**(b) Name of system:** eMED 02.06.00
**(c) System acronym:** eMED
**(d) Bureau**: Bureau of Medical Services
**(e) iMatrix Asset ID Number:** 299
**(f) Child systems (if applicable) and iMatrix Asset ID Number:** N/A
**(g) Reason for performing PIA:**

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

**(h) Explanation of modification (if applicable):** N/A

### 3. General Information

**(a) Does the system have a completed and submitted data types document in Xacta?**
☒Yes ☐No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

**(b) Is this system undergoing an Assessment and Authorization (A&A)?**
☒Yes ☐No

If yes, has the privacy questionnaire in Xacta been completed?
☒Yes ☐No

**(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 provides a standard, rapid, and secure way to enter information into a patient's medical record and enables a patient's medical record 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, a component of eMED, 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 in 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. Additionally, the medevac module of eMED is used to enter administrative and diagnostic information about a patient's medevac. The system enables better tracking of MED evacuees' status and progress and assists in making a clearance decision prior to their return to post. All immunization records administered by MED's Washington, DC health units and those externally administered are 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. For the purposes of this system, Eligible Family Members (EFMs) and their families will be accounted as U.S. government employees as their interaction with eMED is solely due to their relationship to an employee.

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

Medical and demographic information is collected from Department of State candidates, employees, other agency employees and eligible family members from here on referred to as patients. Information that is required for all patients includes:

- First Name
- Last Name
- Date of birth (DOB)
- Gender
- Agency
- Relationship to Employee
- Social Security Number (SSN) (From Foreign Service employees only):

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
- Business and personal email addresses
- Emergency contact information
    - Address
    - Phone number
    - Email address
- Patient ID – an eMED generated unique identifier created during the registration of the patient in the system. eMED also stores:

- Immunization information
- Lab test information
- Medevac information
- Consultations from various specialists
- Clearance level and date

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

- 22 U.S.C. § 4084 – Health Care Program
- 5 C.F.R. Part 792 – Federal Employees Health, Counselling, and Work/Life Programs
- 42 U.S.C. 12112(d) – Medical Examinations and Inquiries

  (B) Information obtained regarding the medical condition or history of the applicant is collected and maintained on separate forms and in separate medical files and is treated as a confidential medical record, except that supervisors and manager may be informed regarding necessary restrictions on the work or duties of the employee and necessary accommodations.

  (ii) first aid and safety personnel may be informed, when appropriate, if the disability might require emergency treatment; and

  (iii) government officials investigating compliance with this chapter shall be provided relevant information on request.
- 5 U.S.C. 79 – Services to Employees

**(f) Is the information searchable by a personal identifier (e.g., name or Social Security number, etc.)?**

☒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):
  February 11, 2015

☐No, explain how the information is retrieved without a personal identifier.

**(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 Office 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 (Consolidate as much as possible):

- Schedule number:
  A-12-001-01a

- Disposition Authority Number:
  DAA-0059-2020-0026-0001- Medical Program Files- Permanent
  DAA-GRS-2017-0010-0012 (GRS 2.7, ITEM 070) – Non-Occupational Individual Medical Case Files – Temporary
  DAA-GRS-2017-0010-0009 (GRS 2.7, ITEM 060) – Occupational Individual Medical Case Files (Long Term) – Temporary

- Length of time the information is retained in the system:
  Patient information will be retained in the system for no less than the period of time specified in Disposition Authorities (25 years) and will be archived rather than destroyed when the retention period has passed.

- 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) On what other entities above is PII maintained in the system?**

☐ Members of the Public
☐ U.S. Government employees/Contractor employees
☐ Other
☒ N/A

**(c) If the system contains Social Security Numbers (SSNs), is the collection necessary?**
☒Yes ☐No ☐N/A

- If yes, under what authorization?
- Executive Order 9397, Federal employment

**(d) How is the PII collected?**

PII is directly provided by the patients. When patients are seeking their initial medical clearance, the PII is collected from the DS-1843, DS-1622, and DS-3057 (OMB APPROVAL NO. 1405-0068) forms submitted to MED/Medical Records (MR) via email to MEDMR@state.gov or via fax to a fax line dedicated to MED MR's fax server. MED /MR registers patients who are not in the system. During the registration process, MR verifies if the patient exists in the Global Talent Management's (GTM) Integrated Personnel Management System (IPMS) view in eMED. If yes, the following PII is copied to patient's record in eMED:

- Last Name
- First Name
- Middle Initial
- SSN
- DOB

If the patient is not found in IPMS, the following PII is manually entered by MR using the information from the submitted forms:

- Last Name
- First Name
- Middle Initial
- DOB

The following are entered for all patients: (DOS and non-DOS)

- Relationship to Employee
- Gender
- Agency

Optional PII:

- Home Address
- Email Address (Personal or Business)

The collected paper and electronic forms with PII are converted by MR to an electronic file that is associated with the patient's ID.

**(e) 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.

**(f) What process is used to determine if the PII is accurate?**

MED verifies the accuracy of the demographic information listed in 4d for Foreign Service personnel and dependents against the Department of State GTM Integrated

Personnel Management system (IPMS). The accuracy of the information is the responsibility of the IPMS system. 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.

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

Demographic and contact information for active patients are checked each time they submit clearance update information, are medically evacuated, or have a clinic appointment. For State Department employees and eligible family members (EFMs), Name, DOB and SSNs are validated against the source information in the IPMS system. The currency of the information is the responsibility of the IPMS system. For non-DOS employees, there is no method to ensure information is current.

**(h) Does the system use information from commercial sources? Is the information publicly available?**

No, the system does not use information from commercial sources. The information is not publicly available.

**(i) How was the minimization of PII in the system considered?**

The eMED system was redesigned in 2006, and at that time, PII that was not necessary was removed and the number of screens that display some information, such as full SSN, was minimized as much as possible. Additionally, SSN is only collected for Foreign Service and Civil Service employees who need a medical clearance for a Temporary Duty Assignment.

## 5. Use of information

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

The PII in eMED is used to establish 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.

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

Yes. The purpose of this system is to accurately document patients' medical clearance reviews and determinations, patients' medevacs, patients' immunizations, and the delivery of health care services No collateral uses exist for the information collected by the system.

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

If yes:

(1) What types of methods are used to analyze the PII?

(2) Does the analysis result in new information?

(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

**(d) If the system will use test data, will it include real PII?**
☐Yes ☒No ☐N/A

If yes, please provide additional details.

## 6. Sharing of PII

**(a) With whom will the PII be shared internally and/or externally? Please identify the recipients of the information.**

Internal: Bureau of Global Talent Management (GTM)

External:

- Anticipated external sharing via eMED may include other agencies ("partners") with personnel that are working under the Chief of Mission authority. These personnel are members of the International Cooperative Administrative Support Services (ICASS) network which is the principal means that the U.S. Government provides and shares the cost of common administrative support needed to ensure effective operations at its more than 200 diplomatic and consular posts abroad.

- Third-party contractors

**(b) What information will be shared?**

Internal: For Department employees and EFMs who are required to have a medical clearance to go to Post, MED shares the clearance date and class (e.g., "Worldwide Available", "Requires Post Approval", "Domestic Assignment Only", "Pending", and "Separation") with GTM. The transmitted information is sent to uniquely identify the patient, and includes last name, first name, MI, DOB, and employee's SSN.

External:

- Agencies: For other U.S. Government agencies whose employees and EFMs are required to have a Department-issued medical clearance to go to Post, MED shares the clearance date and class (e.g., "Worldwide Available", "Requires Post Approval", "Domestic Assignment Only", "Pending", and "Separation") with the agency's designated contact.

- Third-party contractors: In response to court orders received by the Office of the Legal Adviser Office of Employment Law (L/EMP), MED may share the complete patient medical record, to include the PII listed in 3d, to a third-party contractor performing document redaction based on L/EMP's instructions and criteria.

**(c) What is the purpose for sharing the information?**

Internal: DOS employment offers cannot be finalized for patients who are candidates without this information. Patients who are employees or eligible family members cannot travel to a new Post without a valid medical clearance.

External:

- Agencies: The information is shared with other US Government agencies so that they know that an employee is medically cleared for assignment to post.

- Third-party contractors: The information may be shared to allow the third-party contractor to perform medical records redaction based on L/EMP's instructions and criteria.

**(d) The information to be shared is transmitted or disclosed by what methods?**

Internal: There is a secure direct electronic communication connection between the eMED database and the GTM IPMS database. eMED automatically communicates any new data up to Global Talent Management every 20 minutes.

External:

- Agencies: Medical Clearances notifies other U.S. Government agencies about medical clearances of personnel via secure email.
- Third-Party contractor: For legal/redaction review, the information, or records from eMED are securely transmitted via https or Secure File Transfer Protocol (SFTP) to a FedRAMP-authorized secure environment that is accessible by the contractor.

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

Internal: Information is available only to authorized MED and GTM 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, GTM personnel do not have access to personal health information. Thus, a strong segregation of duties is in place.

External:

- Agencies: Information about medical clearances of other U.S. Government employees is only sent to personnel who have been designated by that external agency and is sent using encryption methods.

- Third-Party Contractors: For legal cases, information is available only to the MED contractors who will be performing medical records redaction. The contract with any contractor shall include FAR 52.224-3 clauses that mandate privacy training. The contract outlines the contractor's responsibilities to protect information in accordance with Department policy.

## 7. Redress and Notification

### (a) Is notice provided to the record subject prior to the collection of their information?

Yes. The DS-1843, DS-1622, and DS-3057 forms that are used to obtain this information have an approved Privacy Act Statement (PAS) on the first page. The PASs provided the applicant with notice of what authorizes the Department to collect this information, why the information is being collected, with whom the information will be shared, and whether the information is mandatory. It also provides the applicant with information pertaining to the System of Records Notice (SORN) that governs the collection of this information where the applicant can learn more about how their PII will be utilized.

### (b) Do record subjects have the opportunity to decline to provide the PII or to consent to particular uses of the PII?

☒Yes ☐No

If yes, how do record subjects grant consent?

A patient is made aware of the possible uses and disclosure of their health information on the DS-1843, DS-1622, or DS-3057, and sign the form after providing their information. 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 record subjects not allowed to provide consent?

### (c) What procedures allow record subjects to gain access to their information?

Individuals can submit written requests to the Medical Records (MR) department in the Bureau of Medical Services for copies of the information in their eMED record. Individuals may only request for themselves or minor children. Additionally, the

Department's Privacy Act practices allow for record subjects to gain access to their information by contacting the Department's Freedom of Information Act (FOIA) office for copies of the records retained. Details on this process can be found in the System of Records Notice, STATE-24. The Privacy Act Statement provided to the record subjects points to STATE-24, which addresses the necessary procedures record subjects must follow to gain access to their information.

**(d) Are procedures in place to allow a record subject to correct inaccurate or erroneous information?**

☒Yes ☐No

If yes, explain the procedures.

An individual can inform Medical Records (MR) via MEDMR@state.gov 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. Additionally, individuals can also follow the Department's Privacy Act practices in the System of Records Notice, STATE-24.

If no, explain why not.

**(e) By what means are record subjects notified of the procedures to correct their information?**

The Medical Records SharePoint site informs users that if they believe that their medical record contains inaccurate or erroneous information, they can contact Medical Records. Individuals would communicate with Medical Records via email or phone contact. MR also has their contact information posted on their SharePoint site. Additionally, details on how record subject can correct their information can be found in the System of Records Notice, STATE-24. The Privacy Act Statement provided to the record subjects point to STATE-24, which addresses the necessary procedures record subjects must follow to correct their information.

## 8. Security Controls

**(a) How is all of the information in the system secured?**

The data are contained in an Oracle database that is secured to Department standards (FIPS 140-2 approved), including encryption of data at rest and in transit. eMED users are authenticated via Multi-Factor Authentication (MFA). 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) Explain the different roles that have been created to provide access to the system and the PII (e.g., users, managers, developers, contractors, other).**

- Users: Users are Department of State MED cleared employees (direct hire Foreign Service, Civil Service, contractors, and Medevac Center health unit local employed staff (LES). User roles are further defined by job function (e.g., Medical Clearances, Medical Records, Foreign Programs, Medevac Centers, etc.) allowing the system to tailor user access to only allow access to the PII/PHI that is defined in section 3(d) that is necessary for the User to perform their job.

- Administrators: MED IT staff who are trained to create new accounts, troubleshoot eMED problems, and correct data entry errors reported by users. Administrators provide Tier 2 support and may have full access to the system's PII/PHI as defined in section 3(d). Such access is only employed as necessary to perform job functions and is fully audited.

- Developers: MED IT staff who have database and programming skills to respond to Tier 3 reported problems and to implement approved system changes. Developers provide Tier 3 support and may have full access to the system's PII/PHI as defined in section 3(d). Such access is only employed as necessary to perform job functions and is fully audited.

**(c) Describe the procedures established to limit system and data 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 Department 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 (username) 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 username 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.

**(d) How is access to data in the system determined for each role identified above?**

- Users: The use of any eMED components by Department MED clinical personnel is dependent upon access control, as determined by supervisors. Access control authorizes individual, module-specific access rights upon valid user authentication. User access is terminated when Administrators are notified by the supervisor of a users' termination, or access automatically terminates if a user's OpenNet account is disabled or deleted.

- Administrators: To support MED staff, eMed system administrators have access to all system modules via eMed administrator accounts. They will be responsible for maintaining the systems and will have elevated privileges. To provide Tier 3 support, MED's database administrators also have elevated privileges and the necessary tools to access eMed's Oracle database directly. Administrator access to the system will be removed once they leave the technical team.

- Developers: Developers typically only need access to "test" data (not real patient data) and only when testing a change in the code behind eMed. Developers work on the functionality of the system. Because of this they require full access to the backend of the system to deal with any technical difficulties that may arise. Once developers rotate out of MED IT their access to the system will be terminated.

**(e) What monitoring, recording, auditing safeguards, and other controls 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.

**(f) Are procedures, controls, or responsibilities regarding access to data in the system documented?**

☒Yes ☐No

**(g) Explain the privacy training provided to each role identified in 8(b) that has access to PII other than their own.**

All Users, Administrators, and Developers are required to take the annual Department Cyber Security Awareness Training, PS800 and the biennial mandatory PII Training, PA318 Protecting Personally Identifiable Information. 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.