Billing Code 4710-36

DEPARTMENT OF STATE

[Public Notice: 12065]

Privacy Act of 1974; System of Records

AGENCY: Department of State.

ACTION: Notice of a Modified System of Records.

SUMMARY: The information of the Bureau of Medical Services (MED) system is used and reviewed by medical and administrative personnel to provide health care to the individuals eligible to participate in the medical program, make clearance decisions for individuals eligible to participate in the health care program and for applicants to the Department of State, and as a reference for local medical capabilities. The system also serves to record and monitor the status of the professional credentials of Department of State Foreign Service, Civil Service and Locally Employed Staff healthcare providers.

DATES: In accordance with 5 U.S.C. 552a(e)(4) and (11), this modified system of records will be effective upon publication, except for the routine uses (u), (v), and (w) that are subject to a 30-day period during which interested persons may submit comments to the Department. Please submit any comments by [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]. Unless comments are received that would require a revision, this system of records will become effective on [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: Questions can be submitted by mail, email, or by calling Eric F. Stein, the Senior Agency Official for Privacy, on (202) 485-2051. If mail, please write to: U.S

Department of State; Office of Global Information Systems, A/GIS; Room 4534, 2201 C St., N.W.; Washington, DC 20520. If email, please address the email to the Senior Agency Official for Privacy, Eric F. Stein, at privacy@state.gov. Please write "Medical Records, State-24 " on the envelope or the subject line of your email.

FOR FURTHER INFORMATION CONTACT: Eric F. Stein, Senior Agency Official for Privacy; U.S. Department of State; Office of Global Information Services, A/GIS; Room 4534, 2201 C St., NW; Washington, DC 20520 or by calling (202) 485-2051.

SUPPLEMENTARY INFORMATION: The purpose of this modification is twofold: (1) to consolidate two existing records systems (State-71- Post Capabilities Database and State-24- Medical Records) into a single modified State-24, to accurately reflect the scope of Department medical records; and (2) to reflect the expansion of Medical Records to FedRAMP-authorized Cloud environments. The proposed merged System of Records will include substantive modifications to the following sections: Routine Uses, Categories of Records, Storage, Retrievability, and Record Access Procedures. In addition, the Department is taking this opportunity to make minor administrative updates to the notice in the Security Classification and System Location sections.

SYSTEM NAME AND NUMBER: Medical Records, State-24.

SECURITY CLASSIFICATION: Sensitive But Unclassified.

SYSTEM LOCATION: The Enterprise Server Operations Center (ESOC WEST) in Denver, Colorado. Some records may be stored within a government cloud provided system (Amazon Web Services and Microsoft Azure Gov) and within a FedRAMP authorized government cloud system provided, implemented, and overseen by the

Department's Enterprise Server Operations Center (ESOC), 2201 C Street NW, Washington, DC 20520.

SYSTEM MANAGER: Director for Medical Informatics, Bureau of Medical Services, 2401 E Street, NW, Washington, DC 20522, HerringED@state.gov.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Foreign Service Act of 1980, Sec. 904 (22 U.S.C. 4084); and 5 CFR part 792 (Federal Employees' Health, Counseling, and Work/Life Programs).

PURPOSE(S) OF THE SYSTEM: The records maintained in the systems include Personally Identifiable Information (PII) and Protected Health Information (PHI) and are used to enable MED's practitioners to provide the best medical care possible to a globally dispersed patient population. Records include patients' medical history/records, which are used to provide medical care, adjudicate medical clearances, and support medical evacuations. Additionally, the system describes the medical capabilities available at each Post to support employees under Chief of Mission authority. Moreover, the system also serves to provide medical clearances of applicants to the Department of State. The system also serves to record and monitor the current status of the professional credentials of Department of State Foreign Service, Civil Service and Locally Employed Staff healthcare providers.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Applicants to the Department of State and their family members, U.S. Government employees and their family members, Locally Employed Staff, and any other individuals eligible to participate in the medical program of the U.S. Department of State as authorized by either section 904 of the Foreign Service Act of 1980 (22 U.S.C. 4084) or other applicable legal

authority. The Privacy Act defines an individual at 5 U.S.C. 552a(a)(2) as a United States citizen or lawful permanent resident.

CATEGORIES OF RECORDS IN THE SYSTEM: Categories of records include full name; Social Security number (Department of State Employees and applicants only); date of birth; address; email address; phone number; State Global Identifier (SGID); reports of medical examinations and related documents, images, and other items; reports of treatments and other health services rendered to individuals; immunization records; narrative summaries of hospital treatments; personal medical histories; reports of on-the-job injuries or illnesses; reports on medical evacuation; and/or any other types of individually identifiable health information generated or used in the course of conducting health care operations. This system includes records that contain protected health information and does not include records maintained by the Department of State and/or other employers in their capacity as employers.

This system also includes certain records maintained as part of the Department's Employee Assistance Program pursuant to 5 CFR part 792. The system also includes a directory of MED staff, and professional credentials of MED providers. The directory may include addresses, emails, and phone numbers for direct-hire Foreign Service, Civil Service, and Locally Employed Staff medical personnel. The credentials that are maintained include copies of licenses and certifications (Professional, Clinical, Drug Enforcement Administration (DEA), clinical privileges information, and National Provider Identifier (NPI)). For use by MED clinical staff, the system maintains directories and high-level assessments of the location and quality of medical resources offered in the areas surrounding most Post locations. This system also includes the

medical clearance records of applicants to the Department of State who are in the final stages of their application process and may further include the medical clearance records of their family members.

RECORD SOURCE CATEGORIES: Information contained in these records comes from applicants, patients, hospitals, clinics, laboratories, private medical providers, employers, and medical professionals employed by the Department of State.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES: Medical Records may be disclosed:

A. To another health care provider, a group health plan, a health insurance issuer, or a health maintenance organization for purposes of carrying out treatment, payment, or health care operations;

B. To a parent, guardian or other person acting in loco parentis with respect to the subject of the information;

C. To a health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of the Department of State's medical program, or for such oversight activities as audits; civil, administrative, or criminal proceedings or actions; inspections; and licensure or disciplinary action;

D. To a public health authority (domestic or foreign) that is authorized by law to collect or receive protected health information for the purpose of preventing or controlling disease, injury, or disability, including, but not limited to, the reporting of disease,

injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions;

E. To the U.S. Department of Health and Human Services (HHS), when required by the Secretary of HHS;

F. To a public health authority or other appropriate government authority (domestic or foreign) authorized by law to receive reports of child abuse or neglect;

G. To a person subject to the jurisdiction of the Food and Drug Administration (FDA) with respect to an FDA-regulated product or activity for which that person has responsibility, for the purpose of activities related to the quality, safety, or effectiveness of such FDA-regulated product or activity;

H. To a person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition, to the extent MED is authorized by law to notify such person and as necessary in the conduct of a public health intervention or investigation;

I. To a government authority (domestic or foreign), including a social service or protective services agency, authorized by law to receive reports of abuse, neglect or domestic violence (1) to the extent such a disclosure is required by law; (2) where in the exercise of professional judgment, the disclosure is necessary to prevent serious harm to the individual or other potential victims; or (3) where, if the subject of the information is incapacitated, a law enforcement, or other public official authorized to receive the report, represents that the information sought is not intended to be used against the individual and that an immediate enforcement activity that depends upon

the disclosure would be adversely affected by waiting until the individual is able to agree to the disclosure;

J. To the Department of Justice, as required by law, for the purpose of submitting information to the National Instant Criminal Background Check System;

K. In the course of any judicial or administrative proceeding in response to an order of a court or administrative tribunal;

L. To a law enforcement official (1) as required by law or in compliance with a court order or court-ordered warrant, a subpoena or summons issued by a judicial officer, a grand jury subpoena, or an administrative request, including an administrative subpoena or summons; (2) in response to a request for the purposes of identifying or locating a suspect, fugitive, material witness, or missing person; in response to a request for such information about an individual who is or is suspected to be a victim of a crime; (3) to provide notice of the death of an individual if there is a belief that the death may have resulted from criminal conduct; (4) where it is believed in good faith that such information constitutes evidence of criminal conduct; or (5) in response to an emergency, where it is believed such disclosure is necessary to alert law enforcement to the commission and nature of a crime, the location of such crime or of the victim(s) of such crime, and the identity, description, and location of the perpetrator of such crime;

M. As necessary in order to prevent or lessen a serious and imminent threat to the health or safety of a person or the public or to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat;

N. To authorized federal officials for the conduct of lawful intelligence, counter-intelligence, and other national security activities authorized by the National Security Act (50 U.S.C. 401, et seq.) and other applicable authorities (e.g., Executive Order 12333);

O. To authorized federal officials for the provision of protective services to the President or other persons authorized by 18 U.S.C. 3056 or to foreign heads of state or other persons authorized by 22 U.S.C. 2709(a)(3), or for the conduct of investigations authorized by 18 U.S.C. 871 and 879;

P. To Department of State officials for the purposes of clearance and suitability determinations, including (1) for a national security clearance conducted pursuant to Executive Orders 10450 and 12698; (2) for medical clearance determinations, consistent with the Foreign Service Act, including sections 101(a)(4), 101(b)(5), 504, and 904;

Q. To a medical transcription or translation service for MED's purposes of carrying out treatment or health care operations;

R. To a correctional institution or a law enforcement official having lawful custody of an individual, if the correctional institution or law enforcement official represents that such information is necessary for the provision of health care to such individual, the health and safety of other individuals (including others at the correctional institution), or the administration and maintenance of the safety, security, and good order of the correctional institution;

S. To a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law;

T. To appropriate domestic or foreign government officials (including but not limited to the U.S. Department of Labor), as authorized by and to the extent necessary to comply with laws relating to workers' compensation or other similar programs, established by law, that provide benefits for work-related injuries or illnesses without regard to fault.

U. To appropriate agencies, entities, and persons when (1) the Department of State suspects or has confirmed that there has been a breach of the system of records; (2) the Department of State has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, the Department of State (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department of State efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm

V. To another Federal agency or Federal entity, when the Department of State determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

W. To private sector entities when required as part of U.S. Embassy services or the operations of the State Department Medical Program.

The Department of State periodically publishes in the Federal Register its standard routine uses that apply to all of its Privacy Act systems of records. These notices appear in the form of a Prefatory Statement (published in Volume 73, Number 136, Public Notice 6290, on July 15, 2008). All these standard routine uses apply to Medical Records, State-24.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: Records are stored electronically. A description of standard Department of State policies concerning storage of electronic records is found at https://fam.state.gov/FAM/05FAM/05FAM0440.html.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Patient records are retrievable by individual name and/or date of birth, or patient identification number. MED practitioner records are retrieval by name or Post. Post capability records are retrievable by Post name.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: Records are retired and destroyed in accordance with published Department of State Records Disposition Schedules as approved by the National Archives and Records Administration (NARA) and outlined at https://foia.state.gov/Learn/RecordsDisposition.aspx . Additionally, patient information will be retained in the system for no less than the period of time specified in Disposition Authorities and will be archived rather than destroyed when the retention period has passed. Medical Program Files (permanent) will be transferred to the National Archives 25 years after the end of the calendar year in which the file was last updated. Non-Occupational Individual Medical Case Files (temporary) will be archived by MED no earlier than 10 years after the most recent encounter. Occupational Individual Medical

Case Files (long term – temporary) will be archived by MED no earlier than 30 years after employee separation or when the Official Personnel Folder is destroyed, whichever is longer. More specific information may be obtained by writing to the following address: U.S. Department of State; Director, Office of Information Programs and Services; A/GIS/IPS; 2201 C Street, N.W., Room B-266; Washington, DC 20520.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: All Department of State network users are given cyber security awareness training which covers the procedures for handling Sensitive but Unclassified (SBU) information, including personally identifiable information (PII). Annual refresher training is mandatory. In addition, all Department OpenNet users are required to take the Foreign Service Institute distance learning course instructing employees on privacy and security requirements, including the rules of behavior for handling PII and the potential consequences if it is handled improperly. Before being granted access to Medical Records, a user must first be granted access to the Department of State computer systems.

Department of State employees and contractors may remotely access this system of records using non-Department owned information technology. Such access is subject to approval by the Department's mobile and remote access program and is limited to information maintained in unclassified information systems. Remote access to the Department's information systems is configured in compliance with OMB Circular A-130 multifactor authentication requirements and includes a time-out function. All Department of State employees and contractors with authorized access to records maintained in this system of records have undergone a thorough background security investigation. Access to the Department of State, its annexes, and Posts abroad is

controlled by security guards and admission is limited to those individuals possessing a valid identification card or individuals under proper escort. Access to computerized files is password-protected and under the direct supervision of the system manager. The system manager has the capability of printing audit trails of access from the computer media, thereby permitting regular and ad hoc monitoring of computer usage. When it is determined that a user no longer needs access, the user account is disabled.

The safeguards in the following paragraphs apply only to records that are maintained in government-certified cloud systems. All cloud systems that provide IT services and process Department of State information must be specifically authorized by the Department of State Authorizing Official and Senior Agency Official for Privacy.

Information that conforms with Department-specific definitions for Federal Information Security Modernization Act (FISMA) low, moderate, or high categorization are permissible for cloud usage and must specifically be authorized by the Department's Cloud Program Management Office and the Department of State Authorizing Official. Specific security measures and safeguards will depend on the FISMA categorization of the information in a given cloud system. In accordance with Department policy, systems that process more sensitive information will require more stringent controls and review by Department cybersecurity experts prior to approval. Prior to operation, all Cloud systems must comply with applicable security measures that are outlined in FISMA, FedRAMP, OMB regulations, National Institute of Standards and Technology's (NIST) Special Publications (SP) and Federal Information Processing Standards (FIPS) and Department of State policies and standards.

All data stored in cloud environments categorized above a low FISMA impact risk level must be encrypted at rest and in-transit using a federally-approved encryption mechanism. The encryption keys shall be generated, maintained, and controlled in a Department data center by the Department key management authority. Deviations from these encryption requirements must be approved in writing by the Department of State Authorizing Official. High FISMA impact risk level systems will additionally be subject to continual auditing and monitoring, multifactor authentication mechanism utilizing Public Key Infrastructure (PKI) and NIST 800 53 controls concerning virtualization, servers, storage, and networking, as well as stringent measures to sanitize data from the cloud service once the contract is terminated.

RECORD ACCESS PROCEDURES: Individuals who wish to gain access to or amend records pertaining to themselves should write to U.S. Department of State; Director, Office of Information Programs and Services**;** A/GIS/IPS; 2201 C Street, N.W., Room B-266; Washington, DC 20520. The individual must specify that he or she wishes the Medical Records to be checked. At a minimum, the individual must include: full name (including maiden name, if appropriate) and any other names used; current mailing address and zip code; date and place of birth; notarized signature or statement under penalty of perjury; a brief description of the circumstances that caused the creation of the record (including the city and/or country and the approximate dates) which gives the individual cause to believe that Medical Records include records pertaining to the individual. Detailed instructions on Department of State procedures for accessing and amending records can be found on the Department's FOIA website at https://foia.state.gov/Request/Guide.aspx.

Further, patients can access their medical records through the patient portal, My Global Health (MGH). Patients can seek a printed copy of their medical records by submitting a request to Medical Records, Bureau of Medical Services (address above). Parents may also request medical records of dependent children. At a minimum, the individual requesting a copy of his or her medical records must include the following: name, date and place of birth, current mailing address and zip code, signature, a brief description of the circumstances that may have caused the creation of the records that are the subject of the request, and the approximate date(s) of those records.

CONTESTING RECORD PROCEDURES: Individuals who wish to contest record procedures should write to U.S. Department of State; Director, Office of Information Programs and Services**;** A/GIS/IPS; 2201 C Street, N.W., Room B-266; Washington, DC 20520.

NOTIFICATION PROCEDURES: Individuals who have cause to believe that the Bureau of Medical Services might have medical records pertaining to them and want to request a copy of those medical records should write to write to U.S. Department of State; Director, Office of Information Programs and Services**;** A/GIS/IPS; 2201 C Street, N.W., Room B-266; Washington, DC 20520. The individual must specify that he/she wishes the Medical Records to be checked. At a minimum, the individual must include: full name (including maiden name, if appropriate) and any other names used; current mailing address and zip code; date and place of birth; notarized signature or statement under penalty of perjury; a brief description of the circumstances that caused the creation of the record (including the city and/or country and the approximate dates) which gives

the individual cause to believe that Medical Records include records pertaining to the individual.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: None.

HISTORY: Post Capability Database (State-71) - previously published at 74 FR 65586; Medical Records (State-24) - previously published at 74 FR 24891.

Eric F. Stein,

Deputy Assistant Secretary,

Global Information Services (A/GIS),

Department of State.