National Aeronautics and Space Administration

Privacy Impact Assessment (PIA)

PIA Entry Name: Electronic Health Record System

OFC OF CHIEF HEALTH & MEDICAL OFFIC

NASA Point of Contact: Michaud, Vincent J

Phone Number: 202.358.4719

E-mail: vincent.michaud-1@nasa.gov

PURPOSE OF THE PRIVACY IMPACT ASSESSMENT

The National Aeronautics and Space Administration (NASA) Privacy Impact Assessment (PIA) documents and describes the personally identifiable information (PII) NASA collects and the purpose(s) for which it collects that information; how it uses the PII internally; whether it shares the PII with external entities, and the purposes for such sharing; whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent; how individuals may obtain access to the PII; and how the PII will be protected. NASA publishes its PIAs, as well as its System of Records Notices (SORNs), on the NASA public-facing website, which describes NASA's activities that impact privacy, the authority for collecting personally identifiable information (PII), and the procedures to access and have PII amended or corrected if necessary.

Reviewing Official: Stayce Hoult, Chief Privacy Officer

System Overview: The Office of the Chief Health and Medical Officer (OCHMO) has implemented an Electronic Health Record System (EHRS) in support of the NASA Occupational Health (OH) program. The EHR's objective is to replace the paper-based medical records with electronic health records. This software serves to document OH clinic visits by employees at NASA sites. The EHRS manages clinic visit and industrial hygiene information required by Occupational Safety and Health Administration (OSHA) and the Federal Employees' Compensation Act (FECA).

Privacy / Authorities and Other Requirements	
List all legal authorities and/or agreements that permit the collection of privacy information by the project. Explain how these authorities permit the project and the collection of privacy information. If the project collects Social Security numbers, also identify the specific statutory authority allowing it.	5 USC § 7901 – Health service programs; 51 U.S.C. § 20113;44 U.S.C. § 3101; 42 U.S.C. 2472, 1999 US Code Title 42 - THE PUBLIC HEALTH AND WELFARE CHAPTER 26 - NATIONAL SPACE PROGRAM SUBCHAPTER II - COORDINATION OF AERONAUTICAL AND SPACE ACTIVITIES Sec. 2472 - National Aeronautics and Space Administration 44 U.S.C. 3101; Pub. L. 92-255, the TREAT Astronauts Act Executive Order 14043, Requiring Coronavirus Disease 2019 Vaccination for Federal Employees (Sept. 9, 2021)
The records in the system are covered by an existing published System of Records Notice (SORN).	Existing SORN applicable
The SORN Name and Number.	NASA 10 Health Information Management System (HIMS)

Privacy Act of 1974 / Uses of the Information	
Records on individuals are or will be routinely retrieved from the system by using individual's name or other unique identifier (e.g., personal account number, UUPIC, SSN, etc. is used to locate information about an individual in the application/website/information system/paper record).	Yes

Paperwork Reduction Act / Characterization of the Information	
The record/application/website/information system collects information in a standard way (via forms, surveys, questionnaires, etc.) from 10 or more persons (e.g., members of the public and NASA contractors, and grantees).	Yes

Paperwork Reduction Act / Authorities and Other Requirements

There is an OMB Control Number.	Yes
The OMB Control Number.	OMB-1218-0065; OMB 2700-0174

Privacy / Characterization of the Information

Information is collected on the following:	NASA Contractors Government Employees
Collection contains the following:	Name Date of birth SSN Employment status and/or records Work phone number UUPIC Home mailing address Medical records numbers Medical notes Financial account information Work Mailing Address Home Phone Number
The collection is the minimum necessary to accomplish the purpose of the collection.	Yes
Discuss the intra-Departmental sharing of information. Identify and list the name(s) of any components or directorates within the Department with which the information is shared.	The information is not shared outside of the Department.

Privacy / Uses of the Information

NASA will use the information in the following ways:	The Identifiable Information creates the framework for individual specific medical record files within the electronic health record system (EHRS). The EHRS documents Occupational Health clinic visits by individuals at NASA sites as well as accidents, medical surveillance, and Industrial Hygiene surveillance within NASA centers.
The application/website/information system stores, collects, or maintains Information in Identifiable Form (IIF).	Yes

Consent / Notice

Does the project provide individuals notice prior to the collection of information?	Yes
If no, explain why individuals are not notified prior to collection of information.	
If yes, describe how the notice provided for the collection of information is adequate to inform those impacted.	A Privacy Act Notice is attached to all surveys and request from individuals
Do individuals have opportunities to decline to provide information, or opt out of the project?	Yes
If yes, describe the process. If this is not an option, explain why not.	For requests that allow the individual an option, users are provided with a questionnaire that gives the user the ability to decline
Do individuals have opportunities to consent to specific/targeted uses of their information?	No
If yes, describe the process. If this is not an option, explain why not	how the information is going to be used is decided by clinic staff
The IIF is collected	Mandatory
There is a process in place for the following:	
Ensuring consent is obtained from the individuals whose IIF is stored, collected, or maintained.	Yes
Are individuals provided with notice that they have opportunities to consent to uses, decline to provide information, or opt out of the project?	Yes
If yes, describe the process. If no, explain why not.	The identifiable information used to establish the foundation records within this system is provided by individuals through the Office of Human Resources upon initial employment, and is derived from the NASA Enterprise Directory database, which results in continuous updates of the information automatically maintaining consistency and accuracy of the information. Information contained in EHRS is further managed and maintained in accordance with NASA System of Records Notice, 10HIMS.
Are individuals notified of the consequences of providing information?	Yes
If yes, describe the process. If no, explain why not.	Consequences of Failure to Provide Information is indicated in the Privacy Act Notice

Data Retention	
Explain how long each type of information is retained. Include a justification for the retention period of each information type and how/why that period is necessary to the mission/project.	NASA Records Retention Schedule (NRRS) 1/126C.1, NRRS 1/127A.2, NRRS 1/127B.1, NRRS 1/127B.2, NRRS 1/127C.1, NRRS 1/127C.2, NRRS Schedule 8, NRRS 2/15A, NRRS 2/15A.2, NRRS 2/15B, NRRS 2/15E

Information Sharing

Is information shared outside of the organization as part of the normal agency operations?	Yes
Identify who the information is shared with, how the information is accessed, and how it is to be used.	(1) to external medical professionals and independent entities to support internal and external reviews for purposes of medical quality assurance; (2) to private or other government health care providers for consultation, referral, or mission medical contingency support; (3) to the Office of Personnel Management, Occupational Safety and Health Administration, and other Federal or State agencies as required in accordance with the Federal agency's special program responsibilities; (4) to insurers for referrals or reimbursement; (5) to employers of non-NASA personnel in support of the Mission Critical Space Systems Personnel Reliability Program; Additional routine uses may be found in Gov 10 Health Information Management System (HIMS)
Describe how the external sharing noted in the previous question is compatible with the SORN noted in PIA-02.	external sharing used for consultation

Redress

What are the procedures that allow individuals to access their information?	Access to information is provided in accordance with the Privacy Act Additionally, instructions can be found in section 200 of eCFR part 1212 Updated by (EN)
What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?	Correction of inaccurate or erroneous information is in accordance with the Privacy Act Additionally, instructions can be found in section 300 of eCFR part 1212 Updated by (EN)
How does the project notify individuals about the procedures for correcting their information?	the Privacy Act Notification provides instruction for correcting information.

Auditing and Accountability

How does the project ensure that the information is used in accordance with stated practices in this PIA?	Regular monitoring of information and updates to the Privacy Impact Assessment
Describe what privacy training is provided to users either generally or specifically relevant to the project.	Every NASA employee is required to complete security awareness training and is tested at least annually in compliance with NASA policies. This training is entitled, Annual Information Security

	and Privacy Awareness Training, and is coordinated by NASA HQ CSPD.
What procedures are in place to determine which users may access the information and how does the project determine who has access?	Employees are granted a user account with role restrictions specifically based on their job capacity and their geographic location.
How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within the department and outside?	An updated *System Security Plan* and an updated *Authorization To Operate* would have to be levied in order for different use of this information as explained in this PIA

Security Controls / Characterization of the Information	
Monitor and Response to privacy and/or security incidents policies.	Yes

Security Controls / Auditing and Accountability	
Technical controls (safeguards) are in place to minimize the possibility of unauthorized access, use, or dissemination of the IIF in the application/ website/ information system/ cloud system.	Yes
Access controls.	Yes

Information Sharing Practices / Characterization of Information	
The application/website/information system/cloud systems collects IIF from other resources (e.g., databases, websites).	Yes
The application/website/information system/cloud system populates data for other resources (e.g., databases, websites, or external agencies, people, or organizations).	Yes

Accessibility, Redress, Complaints / Characterization of the Information	
There is a process in place for periodic reviews of IIF in the system to ensure data integrity, availability, accuracy, and relevance.	Yes

Web Measurement and Customizing Technology / Characterization of the Information	
The Application/Website/Information System Utilizes Web Measurement and Customization Technology (Cookies/Persistent Tracking).	No

Agency Privacy Manager (APM):

Guerin, Michael D
HARRIS HOULT, STAYCE D
Kostka, Paul A
Midulla, Laura P
Montasser, Ali S
Scholz, Matthew C

APM Review Decision: Concur

APM Review Date: 08/08/2022

Chief Privacy Officer (CPO):

HARRIS HOULT, STAYCE D

CPO Review Decision: Concur

CPO Review Date: 01/14/2025

_____
CPO Digital Signature

NASA Senior Agency Information Security Officer (SAISO):

Witt, Michael

SAISO Review Decision: Concur

SAISO Review Date: 02/25/2025

NASA Senior Agency Official for Privacy (SAOP):

SEATON, JEFFREY M

SAOP Review Decision: Approve

SAOP Review Date: 03/21/2025