National Science Foundation

Privacy Impact Assessment

for the

Health Program Records

September 20, 2021

1. CONTACT INFORMATION

System Owner
Name: Sarita Marshall
Title: Branch Chief, Pay and Benefits Services
Directorate/Division: Division of Human Resource Management
Telephone Number: (703) 292-8767
Email: Samarsha@nsf.gov

2. GENERAL SYSTEM INFORMATION

1. Name of collection or system: **Health Program Records (NSF-79)**

2. Description of system or electronic collection of information and its purpose.

   Health Program Records contain medical and health related information collected from NSF staff[1] and visitors who use the services of the NSF Health Unit and/or other NSF health programs. Such services may include routine well visits, occupational health, travel clearances, immunizations, and health assessments.

   The Health Program Records system covers any individual who receives care at the NSF Health Unit or by Health Unit staff, or other NSF health programs. Covered individuals may include NSF federal employees, individuals working in the NSF facility or on official NSF business, including Intergovernmental Personnel Act (IPA) assignees, Visiting Scientists, Engineers, and Educators (VSEEs), NSF contractors, non-NSF government personnel or contractors, interns, fellows, volunteers, and visitors to NSF headquarters.

3. What is the purpose of the system or electronic collection of information?

   Information in this system of records is collected and maintained to document an individual's utilization of health services provided by the NSF Health Unit and other NSF health programs. The system includes the following data to:

   - Ensure proper evaluation, diagnosis, treatment, and referral to maintain continuity of care
   - Maintain a medical history of care received by the individual
   - Plan for further care of the individual
   - Communicate among health care members who contribute to the individual's care
   - Maintain a legal document of health care rendered.
   - Coordinate with other federal, state and local agencies when responding to health emergencies
   - Comply with laws regarding the reporting of communicable disease

[1] NSF staff includes Federal employees, Intergovernmental Personnel Act (IPA) assignees, Visiting Scientists, Engineers, and Educators (VEEs), NSF contractors, non-NSF government personnel or contractors, interns, fellows, volunteers.

- Address personnel matters such as requests for reasonable accommodations or travel clearances.

4. Requested Operational Date?

   The estimated date the system will begin operation and the collection of PII is October 2021.

5. Does the collection create a new Privacy Act System of Records Notice (SORN), or is the PII collection covered by one or more existing SORNs? If so, name the SORN.

   NSF-79 Health Program Records is a new SORN.

6. What specific legal authorities, arrangements and/or agreements require collection?

   - 5 U.S.C. 7901, which authorizes the head of a federal agency to establish "a health service program to promote and maintain the physical and mental fitness of employees…,"
   - National Science Foundation Act of 1950 (Public Law 507-81)

3. PII IN THE SYSTEM

1. What PII is to be collected, used, disseminated, or maintained in the system or collection?

   The Health Program Records system will contain personal and medical information from NSF staff and visitors who use the services of the NSF Health Unit or other NSF health programs. Such services may include routine well visits, occupational health, travel clearances, immunizations, and health assessments.

   They system contains health screening data, patient medical records, and other information provided to the Health Unit during the course of patient intake and care, and/or information provided to other NSF health programs that NSF may participate in. These records may include personal data such as:

   - Name
   - Social Security Number
   - Date of birth
   - Address
   - Telephone number
   - Email address
   - Emergency contact information
   - Information about and obtained from and individual's physician
   - Medical history
   - Biographical data including about family members
   - Examination, diagnostic, assessment, and treatment data
   - Laboratory findings
   - Nutrition and dietetic files
   - Nursing notes
   - Immunization records

- Vaccination records
- Prescription information.

2. What are the sources of the PII?

   Information in this system of records comes from the individual to whom it applies; laboratory reports and test results; health unit physicians, nurses, and other medical technicians who have examined, tested, or treated the individual; the individual's personal physician; other federal employee health units; and other federal, state, and local agencies.

3. What technologies will be used to collect the PII?

   A new electronic record keeping system will support electronic registration of new patients as well as the capability for patients 24/7 access their medical records.

4. ATTRIBUTES OF THE DATA (USE AND ACCURACY)

1. Describe the uses of the PII.

   NSF intends to collect the information to assist NSF with maintaining a safe and healthy workplace, to allow the NSF Health Unit to provide medical evaluation and treatment of patients, comply with laws and policies regarding the reporting of communicable diseases, support personnel related matters, and allow NSF staff to participate in NSF health programs.

2. Does the system perform any strictly analytical functions on the PII?

   The system does not perform any analytical functions on the PII.

3. How will the accuracy of the PII collected from individuals or derived by the system be ensured?

   Information in this system of records comes from the individual to whom it applies; laboratory reports and test results; health unit physicians, nurses, and other medical technicians who have examined, tested, or treated the individual; the individual's personal physician; other federal employee health units; and other federal, state and local agencies.

   Records in this system are safeguarded in accordance with applicable law, rules, and policies, including all applicable NSF automated systems security and access policies. Strict controls have been imposed to minimize the risk of compromising the information that is being stored. Access to the computer system containing electronic records in this system is limited to those individuals who have a need to know (including medical personnel under a contract agreement) the information for the performance of their official duties. These records are maintained in a secure password-protected environment. All users are required to take annual NSF IT Security and Privacy Awareness Training, which covers the procedures for handling Sensitive but Unclassified Information, including personally identifiable information (PII).

5. SHARING PRACTICES

1. Describe any sharing of the PII with internal or external organizations.

   Data retrieved from the site will be shared with the standard routine uses as listed in SORN NSF-79.

   To reduce the risk to individual privacy, NSF minimizes dissemination of the information it maintains including within the agency. For example, only NSF staff who have a need to know the information to assess a request for a reasonable accommodation will be given access to the information for that purpose.

2. How is the PII transmitted or disclosed to the internal or external organization?

   Disclosures are accomplished using secure electronic transmissions accepted as adequate for use by all federal agencies.

   The means of disclosure to other external organizations or persons permitted under the authority of the Privacy Act or FOIA will depend on the circumstances of the records request presented to NSF.

3. How is the shared PII secured by external recipients?

   Disclosures under the authority of the Privacy Act are considered on a case-by-case basis, and most relate to a records request from another Executive Branch agency. In such cases, the requesting agency is obligated to protect the information under information security requirements established by the Federal Information Security Management Act (FISMA).

6. NOTICE TO INDIVIDUALS TO DECLINE/CONSENT USE

The following questions address actions taken to provide notice to individuals of their right to consent/ decline to collection and use of information (other than required or authorized uses) and how individuals can grant consent.

1. How does the program or collection provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

   Notice prior to collection of PII from NSF employees and visitors is accomplished by the several means required by federal statute. These means of notice are as follow:

   - For information collected by NSF from participants, notice is provided in the Federal Register in the form of a new or amended Paperwork Reduction Act information collection request.
   - Notice of the Privacy Act systems of records listed in paragraph 2(6) of this PIA is published in the Federal Register. These constitute notice required by the Privacy Act at 5 U.S.C. 552a(e)(4) of the general character and existence of records.

- Website privacy policies are located on the NSF.gov website. These policies constitute notice required by the Privacy Act at 5 U.S.C. 552a(e)(3) and by Section 208(c) of the E-Government Act.

- This PIA, published on the NSF public website, satisfies the notice requirement of Section 208(b) of the E-Government Act.

2. Do individuals have the opportunity and/or right to decline to provide any or all PII?

   Individuals have the opportunity and right to decline providing data.

3. Do individuals have the right to consent to particular uses of their PII?

   Individuals have the right to consent to uses of data.

7. ACCESS TO DATA (ADMINISTRATIVE AND TECHNICAL CONTROLS)

1. What categories of individuals will have lawful access to the system?

   Only authorized Human Resource personnel, or NSF personnel on a "need to know" basis, will be granted access permission by the Branch Chief - Pay and Benefits Services.

2. How is permissible access by a user determined? Are procedures documented?

   Individuals seeking to access information about themselves contained in this system are required to follow the procedures found at 45 CFR part 613.

3. What auditing measures/controls and technical safeguards are in place to prevent exposure or misuse of PII by authorized users, e.g., record browsing, extraction?

   NSF information system owners determine audited and auditable events for each information system based on activities and information that are deemed significant and relevant to business needs and the security of the system.

   Information System Owners use the Mandatory Security Audit Event Requirements outlined in the NSF Audit Events Procedure to identify the frequency of audited events and determine the level of logging required for each mandatory audit event.

   NSF audit records involve the logging and monitoring of activities related to the access and modification of sensitive information or configuration changes. Audit records maintain a record of system activity that can establish what type of event occurred, when (date and time) the event occurred, where the event occurred, the source of the event, the outcome (success or failure) of the event, and the identity of any user/subject associated with the event and facilitates the investigation of outages or possible security violations.

   Only authorized users have access to administer and monitor information in the application.

4. Describe privacy training provided users, general or specific, relevant to the program or system?

NSF maintains a system use notification banner prior to logging on to the NSF Network.

All Intergovernmental Personnel Act (IPA) employees, federal employees, visiting scientists, and contractors must complete annual IT Security and Privacy Awareness Training. IT Security and Privacy Awareness Training discusses such topics as recognizing types for sensitive information that must be protected at NSF (e.g., protected health information, proprietary , Privacy Act, and confidential financial records); the various Federal laws and guidance that relate to the protection of privacy in individuals and business; and an introduction to NSF's privacy policies (e.g., Information Technology Security and Privacy Awareness Training Policy, Policy Regarding the Privacy of Sensitive Information, and Policy on Reporting the Breach of Personally Identifiable Information).

5. Describe the extent to which contractors will have access to the system.

   NSF contractors do not have access to the system. Access to the system is limited to authorized users on a "need to know" basis. The system has restricted access.

6. Describe the retention period for the personal records in the system.

   All data maintained by this system of records are retained and destroyed in accordance with the NARA Records Schedule 2.7; Item 010 (clinic scheduling records); Item 060, 061, and 062 (occupational individual medical case files); and Item 070 (non-occupational individual medical case files).

7. What is the disposition of the personal records at the end of the retention period?

   All data maintained by this system of records are retained and destroyed in accordance with the NARA Records Schedule 2.7; Item 010 (clinic scheduling records); Item 060, 061, and 062 (occupational individual medical case files); and Item 070 (non-occupational individual medical case files).

8. SECURITY

1. Is the PII secured in accordance with FISMA requirements?

   The NSF Network has an Authorization to Operate for a moderate impact system in accordance with FISMA and National Institute of Standards and Technology (NIST) requirements.

   Records in this system are safeguarded in accordance with applicable law, rules, and policies, including all applicable NSF automated systems security and access policies. Strict controls have been imposed to minimize the risk of compromising the information that is being stored. Access to the computer system containing electronic records in this system is limited to those individuals who have a need to know (including medical personnel under a contract agreement) the information for the performance of their official duties. These records are maintained in a secure password-protected environment. All users are required to take annual NSF IT Security and Privacy Awareness Training, which covers the procedures for handling Sensitive but Unclassified Information, including personally identifiable information (PII).

9. PRIVACY ANALYSIS

NSF operates applications in accordance with security procedures required by federal law and policy to ensure that information is appropriately secured. NSF maintains a continuous monitoring program, identifies appropriate security controls to protect against identified risks, and implemented those controls. NSF performs monitoring, testing, and evaluation of controls on a regular basis to ensure controls continue to work properly.

Key security controls include:

- NSF requires the use of PIV enabled single sign-on for access to applications on the NSF network.
- NSF staff sign Rules of Behavior that include access to sensitive information.
- Systems limit access to only those who have the need to know and access is recertified annually.
- NSF implements encryption for data in transit and data at rest.
- NSF has a comprehensive incident and privacy breach response program to respond to potential breaches of privacy information. The incident response procedure is tested twice a year.