National Science Foundation

Privacy Impact Assessment

for the

NSF Staff and Visitor Medical Information

September 2021

1. CONTACT INFORMATION

System Owner
Name: Sarita Marshal
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:

   NSF-78 NSF Staff and Visitor Medical Information

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

   NSF Staff and Visitor Medical Information[1] may collect workplace safety and personnel information in response to a health-related declaration of a national emergency by the United States President, the Secretary of the Department of Health and Human Services (HHS) or other designated federal official, or a designated state official.

   NSF may collect this information in response to a declaration of public health emergency by the Secretary of HHS. Under section 319 of the Public Health Service Act, the Secretary of HHS may declare that: (a) A disease or disorder presents a public health emergency; or (b) that a public health emergency, including significant outbreaks of infectious disease or bioterrorist attacks, otherwise exists. When the Secretary of HHS determines that a public health emergency exists, NSF must respond to protect the health of its workforce. NSF's response will depend on the nature of the particular public health emergency but may include collecting information from NSF staff and visitors.

   NSF may also collect this information when it determines that the spread of a communicable disease presents a significant risk of substantial harm to the health of NSF staff or visitors. NSF will consider any public health emergency declared by state or local officials in making such a determination. In other circumstances, even in the absence of a health-related declaration of national emergency or declaration of public health emergency (HHS or state level), NSF may collect this information where it determines that the spread of a communicable disease presents a significant risk of substantial harm to the health of NSF staff or visitors.

[1] Contact tracing is defined as the identification, monitoring, and support of an affected individual (an individual in the NSF facility with confirmed or probable exposure to a public health emergency contaminant), and identification and contact of a potentially affected individual (an individual who was in contact with an affected individual or exposed to a public health emergency contaminant while in the NSF facility or at an NSF-sponsored event outside of the NSF facility).

The purpose of the collection of NSF Staff and Visitor Medical Information is to protect the health of NSF staff[2] and visitors who seek to enter the NSF facility and/or were physically present in the facility and came in close proximity to or had physical contract with NSF staff and/or visitors who, at the time, were infected or had symptoms of infection with a communicable disease.

This system covers 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, and volunteers. Other categories of individuals covered by the system include visitors to the NSF facility and potentially affected individuals at NSF-sponsored events outside of the NSF facility or otherwise present during official NSF business. The system also covers individuals listed as emergency contacts for such individuals.

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

   For workplace safety, NSF Staff and Visitor Medical Information information will be used to:

   - Protect individuals in the NSF facility and NSF-sponsored events from risks associated with a public health emergency
   - Plan and respond to workplace and personnel flexibilities needed during a public health emergency
   - Facilitate NSF's cooperation with public health authorities
   - Perform contact tracing investigations of and notifications to NSF staff and visitors known or suspected of exposure to communicable diseases who came in close physical proximity to or had physical contact with other persons while working in or visiting the NSF fac
   - Comply with laws and policies regarding the reporting of communicable diseases, support personnel related matter
   - Comply with Occupational Safety and Health Administration (OSHA) recordkeeping requirements

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-78 NSF Staff and Visitor Medical Information is a new SORN.

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

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

   Legal authority for operating the system include:

   - Occupational Safety and Health Act (OSHA) of 1970, Public Law 91-596, Section 19(a) (29 U.S.C. 668(a))
   - Executive Order 12196 (Occupational Safety and Health Programs for Federal Employees), 5 U.S.C. 7902(d); 29 U.S.C. 668, 29 CFR part 1904, 29 CFR 1910.1020, and 29 CFR 1960.66
   - Executive Order 13991 (Protecting the Federal Workforce and Requiring Mask-Wearing); OMB Memorandum M-21-15 , COVID-19 Safe Federal Workplace: Agency Model Safety Principles
   - OMB Memorandum M-21-25, Integrating Planning for A Safe Increased Return of Federal Employees and Contractors to Physical Workplaces with Post-Reentry Personnel Policies and Work Environments
   - Updated COVID-19 Workplace Safety: Agency Model Safety Principles, issued by the Safer Federal Workforce Task Force
   - 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?

   Health and personal information collected may contain:
   - Name
   - Address
   - Work or personal telephone number(s)
   - Email address(es)
   - Organization (directorate/division)
   - Birth date
   - Social Security Number
   - Medical reports
   - Assessments
   - Vaccination status
   - Testing status (where and when it occurred, status of results)
     - Test type
     - Test results
     - Disease type
   - Health status
   - Approximate date of exposure

- Last date physically present in the NSF facility or at an NSF-sponsored event
- Name of facility visited (if outside of the NSF facility)
- Areas of the NSF or other facility (if an NSF event outside of the NSF facility) traversed
- Areas and object touched
- Workplace contacts
- Names of persons who had physical contact with or was in prolonged close physical proximity to infected/potentially infected persons,
    - Extended proximity event time and date
    - Number of events
    - Number of individuals in an event
    - Number of individuals at location
- Dates and location of domestic and international travel
- Related information and documents collected for the purpose of screening and contact tracing, including attestations regarding vaccination, testing, and treatment status.

2. What are the sources of the PII?

   Records are obtained through paper forms, interviews, or electronically from NSF staff, visitors, or individuals who attend an NSF-sponsored event. With regard to contact tracing, information may be collected from individuals infected or potentially infected while physically present in the NSF facility or at an NSF-sponsored event, other individuals with whom an infected or potentially infected individual had close contact, other federal or state agencies, physicians (as allowed by law or with consent from the individual), visitors or their employers, and NSF staff and visitors who maintain (manually or electronically) a log or report of their close physical contacts (and the duration of that contact) while in the NSF facility to individuals designated by NSF.
   Information is also collected from security systems monitoring access to Agency facilities (such as video surveillance and key card logs), human resources systems, emergency notification systems, and federal, state, and local agencies assisting with the response to a public health emergency.

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

   ServiceNow is a FedRAMP certified Software as a Service (SaaS) with a current Authorization to Operate (ATO) and categorized as MODERATE however, the NSF system is configured for HIGH since December 2019. ServiceNow is used by NSF's Human Resource Management to create and track human resource-related inquires and protected health information. The information collected is used for internal purposes only to manage IT services and for the Human Resource division to manage NSF personnel.

4. ATTRIBUTES OF THE DATA (USE AND ACCURACY)

1. Describe the uses of the PII.

   NSF intends to collect PII, including medical information to conduct health screening to:

   - Identify persons who have or may have been exposed to or infected with a communicable disease (e.g., to reduce risk by allowing them to work from home or use leave, as needed).

- Help reduce the risk that individuals with symptoms consistent with a communicable disease who enter the NSF facility or event and infect NSF staff and/or visitors with a communicable disease.

- Identify other NSF staff and/or visitors who were present in the NSF facility or another facility hosting an NSF-sponsored event or in close proximity to or had physical contact with NSF staff and/or visitors who, at the time, were infected or had symptoms of infection with a communicable disease.

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 users as listed in SORN NSF-78.

   To reduce the risk to individual privacy, NSF minimizes dissemination of the information it maintains. For example, if NSF staff or visitor tests positive for a communicable disease and reveals this information to NSF (or NSF acquires this information from another source), their identity will not be disclosed to other persons with whom they came in close physical contact unless otherwise authorized by law.

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 participants in an NSF assistance program 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 conducts a risk assessment of applications, identifies appropriate security controls to protect against identified risk, and implements those controls. NSF Information Security and Privacy Continuous Monitoring (ISCM) activities incorporate compliance with FISMA and ongoing operational security throughout the system's lifecycle. NSF performs monitoring, testing, and evaluation of controls on a regular basis to ensure controls continue to work properly.

NSF established a continuous monitoring approach that assesses the security state of information systems based on FISMA and NIST security requirements and guidance.

Continuous monitoring activities consist of program activities and operational and technical controls (automated and manual) to provide adequate security for NSF systems.

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.