US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

04/05/2024

OPDIV:

NIH

Name:

Synthesize, Analyze, Adjudicate, & Vet Information

PIA Unique Identifier:

P-5996245-859519

The subject of this PIA is which of the following?

Major Application

Identify the Enterprise Performance Lifecycle Phase of the system.

Operations and Maintenance

Is this a FISMA-Reportable system?

Yes

Does the system include a Website or online application available to and for the use of the general public?

No

Identify the operator.

Agency

Is this a new or existing system?

Existing

Does the system have Security Authorization (SA)?

Yes

Indicate the following reason(s) for updating this PIA.

PIA Validation

Describe in further detail any changes to the system that have occurred since the last PIA.

Although the Synthesize, Analyze, Adjudicate & Vet Information (SAAVI) system may contain personally identifiable information (PII), the system does not explicitly collect or require any information from the public. The previous version of the privacy impact assessment (PIA) specifically identified the most commonly received types of personally identifiable information (PII), given the wide variety of potential PII. Whereas, less commonly received PII was encompassed by a general statement.

The updated PIA specifies a broader range of PII that may potentially be collected by the system. This update aims to provide more clarity and transparency to the public regarding the potential collection of PII.

Describe the purpose of the system.

The Synthesize, Analyze, Adjudicate & Vet Information (SAAVI) system electronically manages

(scans, distributes, tracks and disposes of) documents coming to, and assignments originating from, the NIH Director. NIH Executive Secretariat (ES) staff use SAAVI to assign these documents for action or clearance, or disseminate them for information to one or more of the 27 NIH Institutes and Centers (ICs) and 32 offices within the NIH Office of the Director (OD). NIH staff in these offices prepares response documents for signature from the IC Director, the NIH Director, or other high level official in the Department of Health and Human Services (DHHS).

Describe the type of information the system will collect, maintain (store), or share.

Original correspondence is scanned or saved within the system and may contain personal information in the body of the correspondence. Theoretically, the correspondences may contain personally identifiable information (PII). The PII is voluntarily provided by the correspondent. There is no process in place to notify, obtain additional information or further consent after the correspondence has been received. SAAVI does not solicit or collect information for a database. The originator/correspondent voluntarily sends PII in the correspondence they authored to the NIH Director or Deputy Director. SAAVI contains only an image of the document originally submitted. SAAVI does not manipulate the information for another use.

There is no way to anticipate the type of PII in a piece of incoming correspondence, but it may include: name, date of birth, personal telephone numbers, social security numbers, and government identification numbers.

Additionally, some public PII is incidentally and voluntarily submitted by the public. No PII is solicited by the SAAVI system. When feasible, unwarranted PII is redacted from the system.

Users log in to this system using NIH Identity, Credential, and Access Management (IAM) Services which maintains its own unique privacy impact assessment (PIA) on record, including all legal authorities documented. The purpose of IAM Services is to authenticate and authorize all users and computers in a Windows domain type network; assigning and enforcing information security policies for all computers and installing or updating software. IAM Services collects unique user credentials and stores them in an encrypted format. IAM Services are an essential service which facilitates and governs network access to various resources.

Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.

SAAVI electronically manages (scans, distributes, tracks, and disposes of) documents coming to, and assignments originating from, the NIH Director's office. Authorized NIH/ES staff use SAAVI to assign these documents for action or clearance, or disseminate them for information to one or more of the 27 NIH Institutes and Centers (ICs) and 32 offices within the NIH OD.

The primary data stored in SAAVI pertain to the correspondence and can include who it was from, intended for, date of correspondence, keywords for searching, etc. No PII is requested as it pertains to processing correspondence, however the correspondence itself may theoretically contain PII. The PII is voluntarily provided by the correspondent. There is no process in place to notify, obtain additional information or further consent after the correspondence has been received. SAAVI does not solicit or collect information for a database. The originator/correspondent voluntarily sends PII in the correspondence they authored to the NIH Director or Deputy Director. SAAVI contains only an image of the document originally submitted. SAAVI does not manipulate the information for another use.

There is no way to anticipate the type of PII in a piece of incoming correspondence, but it may include: name, date of birth, personal telephone numbers, social security numbers, and government identification numbers.

Additionally, some public PII is incidentally and voluntarily submitted by the public. No PII is solicited by the SAAVI system. When feasible, unwarranted PII is redacted from the system.

Users log in to this system using NIH Identity, Credential, and Access Management (IAM) Services which maintains its own unique privacy impact assessment (PIA) on record, including all legal authorities documented. The purpose of IAM Services is to authenticate and authorize all users and computers in a Windows domain type network; assigning and enforcing information security policies for all computers and installing or updating software. IAM Services collects unique user credentials and stores them in an encrypted format. IAM Services are an essential service which facilitates and governs network access to various resources.

Does the system collect, maintain, use or share PII?

Yes

Indicate the type of PII that the system will collect or maintain.

Social Security Number
Date of Birth
Name
Photographic Identifiers
Driver's License Number
Biometric Identifiers
Mother's Maiden Name
Vehicle Identifiers
E-Mail Address
Mailing Address
Phone Numbers
Medical Records Number
Medical Notes
Financial Accounts Info
Certificates
Legal Documents
Education Records
Device Identifiers
Military Status
Employment Status
Foreign Activities
Passport Number
Taxpayer ID
Login ID
Government identification numbers
The correspondences may contain personally identifiable information (PII). Please note that PII is voluntarily provided by the correspondent and not required by the system.

Indicate the categories of individuals about whom PII is collected, maintained or shared.

Employees
Public Citizens
Business Partner/Contacts (Federal/state/local agencies)
Vendor/Suppliers/Contractors

How many individuals' PII is in the system?

500-4,999

For what primary purpose is the PII used?

Correspondence received may be forwarded to an IC subject matter expert, or the HHS Office of the Secretary, for comment, review, drafting a response, or information purposes. Such correspondence may contain PII.

The system uses IAM for authentication and maintains user credentials in order to control access to the system for the purpose of establishing use and viewing rights in the system.

Describe the secondary uses for which the PII will be used.

Not applicable

Identify legal authorities governing information use and disclosure specific to the system and program.

5 U.S.C. 301; 44 U.S.C. 3101

Are records on the system retrieved by one or more PII data elements?

Yes

Identify the number and title of the Privacy Act System of Records Notice (SORN) that is being use to cover the system or identify if a SORN is being developed.

09-90-1901, HHS Correspondence, Customer Service, and Contact List Records

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

Hardcopy

Email

Online

Other

Government Sources

Within OpDiv

Other Federal Entities

Non-Governmental Sources

Public

Media/Internet

Private Sector

Other

Identify the OMB information collection approval number and expiration date

Not Applicable.

SAVE Approval to solicit, collect, or obtain information from responding to identical questions.

Is the PII shared with other organizations?

Yes

Identify with whom the PII is shared or disclosed and for what purpose.

Describe any agreements in place that authorizes the information sharing or disclosure.

Not applicable

Describe the procedures for accounting for disclosures.

Disclosure may be made to a congressional office from the record of an individual in response to an inquiry from the congressional office made at the request of that individual.

Disclosure may be made from this system of records by the HHS to the Department of Justice, or to a court or other tribunal, when (a) HHS, or any component thereof; or (b) any HHS employee in his or her official capacity; or (c) any HHS employee in his or her individual capacity where the Department of Justice (or HHS, where it is authorized to do so) has agreed to represent the employee; or (d) the United States or any agency thereof where HHS determines that the litigation is likely to affect HHS or any of its components, is a party to litigation or has any interest in such litigation, and HHS determines that the use of such records by the Department of Justice, court or other tribunal is relevant and necessary to the litigation and would help in the effective representation of the governmental party, provided, however, that in each case, HHS determines that such disclosure is compatible with the purpose for which the records were collected.

Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason.

The PII is voluntarily provided by the correspondent. There are no processes in place to notify, obtain additional information or further consent after the correspondence has been received. SAAVI does not solicit or collect information for a database. The originator/correspondent voluntarily sends PII in the correspondence authored to the NIH Director or Deputy Director. SAAVI contains only an image of the document originally submitted. SAAVI does not manipulate the information for any another use.

If SAAVI system users/administrators do not want to provide their user credentials, they are unable to gain access to the system.

Is the submission of PII by individuals voluntary or mandatory?

Voluntary

Describe the method for individuals to opt-out of the collection or use of their PII. If there is no option to object to the information collection, provide a reason.

The PII is voluntarily provided by the correspondent. There are no processes in place to notify, obtain additional information or further consent after the correspondence has been received. SAAVI does not solicit or collect information for a database. The originator/correspondent voluntarily sends PII in the correspondence authored to the NIH Director or Deputy Director. SAAVI contains only an image of the document originally submitted. SAAVI does not manipulate the information for any another use.

If SAAVI system users/administrators do not want to provide their user credentials, they are unable to gain access to the system.

Process to notify and obtain consent from individuals whose PII is in the system when major changes occur to the system.

All information provided is voluntary. It is not received by NIH through the website but rather through email, mail, fax, etc. Only information required to respond to correspondence is retained.

For the purpose of system access, users and administrators are given notice via e-mail when system changes occur and/or privileges are updated or revoked.

Describe the process in place to resolve an individual's concerns when they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate.

Individuals may reach out to the system administrators to reasonably identify the record and specify the information to be contested, and state the corrective action sought and the reasons for the

correction. The right to contest records is limited to information which is incomplete, irrelevant, incorrect, or untimely (obsolete).

Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy.

The NIH Office of the Director Executive Secretariat has Record Managers that schedule, review and dispose of correspondence based on NIH retention policies.

Identify who will have access to the PII in the system and the reason why they require access.

Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.

Access to the system is requested from within the application user interface by an existing user. The system routes the request to the NIH Office of the Director Executive Secretariat (ES) who in turn, provides permission to proceed with verification and approval. Then, access is granted by an authorized system administrator.

In some cases, a Director's signature is required from the IC or Office that made the request before NIH ES will grant the request.

Describe the methods in place to allow those with access to PII to only access the minimum amount of information necessary to perform their job.

By default, all correspondence that is added to the system is only accessible to the NIH Office of the Director, Executive Secretariat and authorized users. Authorized user access is granted on a need to know basis by receiving the correspondence by referral from the Executive Secretariat.

Identify training and awareness provided to personnel (system owners, managers, operators, contractors and/or program managers) using the system to make them aware of their responsibilities for protecting the information being collected and maintained.

The NIH Security Awareness Training course is used to satisfy this requirement. According to NIH policy, all personnel who use NIH applications must attend security awareness training every year. There are five categories of mandatory IT training (Information Security, Counterintelligence, Privacy Awareness, Records Management and Emergency Preparedness). Training is completed on the http://irtsectraining.nih.gov site with valid NIH credentials.

Describe training system users receive (above and beyond general security and privacy awareness training).

Additional training is provided for new users and others by request. Training usually includes an ES overview of correspondence sources and system use in routing and responding to correspondence.

Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices?

Yes

Describe the process and guidelines in place with regard to the retention and destruction of PII.

SAAVI does not specifically collect and retain PII but such information may be in the content of a document or attachment that is uploaded to the system.

Records are retained and disposed pursuant to Records Schedules established by NIH with the approval of the National Archives and Records Administration (NARA). Subject and correspondence files of the Director are covered by Record Schedule Items 11-101, 11-102, and 11-103. Official

Subject Files of the Director (11-101) are transferred to NARA after 15 years under Disposition Authority DAA-0443-2017-0003-0001 and the Schedule of Daily Activities Files of the NIH Director and Principal Deputy Director (11-103) are transferred to NARA after 15 years under Disposition Authority DAA-0443-2017-0003-0003. Working Files within the Subject Files of the Official Subject Files of the Director (11-102) are destroyed after 5 years under Disposition Authority DAA-0443-2017-0003-0002.

Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.

Administrative Controls: SAAVI is not intended to collect PII. However, if any comes in as included in the correspondence, SAAVI keeps an audit trail of all functional areas. The system uses multi-level role-based system access controls that are regularly updated by the business owner and system administrator. NIH employee PII required to use SAAVI is hosted by Center of Information Technology (CIT) where annual security audits are conducted for physical, technical and administrative access. Users have access only to information that is pertinent to their IC.

Technical Controls: The system, in conjunction with its operating environment, uses identification and authentication measures that allow only authorized users to access the system. The database containing the document images are encrypted. The system web site uses Secure Socket Layer (SSL) and Security Logging is activated. The web user interface provides 128-bit encryption and is Public Key Infrastructure (PKI)-enabled. Each user must access NIH Login (IAM) and provide appropriate credentials which subsequently provides token access to SAAVI. Inactivity timeouts result in the user having to re-enter their credentials via NIH Login (IAM).

Physical Controls: Physical records are stored in locked cabinets and deleted documents are shredded. The system provides digital signature capability that uses 2-factor authentication.