US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

11/06/2024

OPDIV:

NIH

Name:

CIT Secure Email File Transfer (SEFT)

PIA Unique Identifier:

P-2911036-130335

The subject of this PIA is which of the following?

Minor Application (stand-alone)

Identify the Enterprise Performance Lifecycle Phase of the system.

Operations and Maintenance

Is this a FISMA-Reportable system?

No

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

Yes

Identify the operator.

Agency

Is this a new or existing system?

New

Does the system have Security Authorization (SA)?

Yes

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

Describe the purpose of the system.

The NIH Secure Email File Transfer (SEFT) is a web-based application that provides a means for the NIH community and external partners to securely share emails and large files with sensitive data (up to 200 gigabytes (GB)), using secure data protocols.

Medical Secure Email File Transfer (MedSEFT) is commissioned by the NIH Clinical Center (CC) as one of their authorized methods for providers/clinicians to directly communicate with patients.

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

The type of data and information that SEFT/MedSEFT will store or maintain, include:
Name
Email
Phone
Date of Birth (DOB)
Mailing address

Employment status
Driver's license number
Mother's maiden name
Education records
Medical Notes
Certificates
Military status
Legal documents
Taxpayer identification (ID)
Passport number
Device identifiers
Photographic identifiers
Demographic data
Vehicle identifiers including license plate information
Employee Records
Training records
Insurance Information
Executable files with extensions of .exe, .jar, .dmg, .pkg, .msi, and .war
Social Security Numbers (SSN), including last 4 digits
Credit Card Numbers (CCNs)
Medical/patient information, Medical Record Number (MRN)
Grant or contract information

Sensitive network and system data/information.
System vulnerability and compliance information
NIH third-party proprietary information
Sensitive network and system data/information
System vulnerability and compliance information
Internet Protocol (IP) Address

Personally identifiable information (PII) and sensitive PII that is collected, maintained and/or stored outside the scope of this PIA is the responsibility of the NIH Institute, Center and/or Office (ICO) and a separate PIA must be prepared. Furthermore, sharing PII is subject to the Privacy Act and should only be disclosed in accordance with the law. Data may become PII or Sensitive PII due to context of use.

CIT has implemented the following security safeguards:
NIH Firewall protection
Multi-Factor Authentication (MFA) requiring more than one method to verify the user's identity.
Files uploaded and downloaded via the website are transmitted with Transport Layer Security (TLS) encryption. Uploaded files are encrypted at-rest using Advanced Encryption Standard (AES) 256-bit encryption. This software conforms to Federal Information Processing Standards (FIPS 140-2 “Security Requirements for Cryptographic Modules.”).

User Access
Users log in to this system using the NIH Identity, Credential, and Access Management (IAM) Services which maintains its own unique 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. The IAM Services collect unique user credentials and stores them in an encrypted format. The IAM Services are an essential service which facilitates and governs network access to various resources.

For individuals internal to NIH, such as business partners, collaborators, and researchers; the system uses NIH Federated Services, a centralized authentication hub for web-based applications at NIH, instead of storing a user's login credentials. NIH Federated login enables users to use a single authentication method via an individual's parent organization. After the system owner approves access to an individual and registers their parent organization's identity provider, individuals are redirected to their parent organization's identity provider for credentials. NIH Federation Services resides within the NIH IAM Services.

External users can only access and reply to emails sent to them by a NIH or Health Resources and Services Administration (HRSA) user. External users cannot initiate new file transfers from SEFT. External users must contact the NIH Information Technology (IT) Service Desk to set up an account in order to retrieve and read SEFT messages.

SEFT and MedSEFT are operated and managed by the Center for Information Technology (CIT) Unified Communication and Collaboration (UCC).

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

The NIH SEFT is a web-based application that provides a means for the NIH community and external partners to securely share emails and large files with sensitive data (up to 200 GB), using secure data protocols. MedSEFT is commissioned by the NIH CC as one of their authorized methods for providers/clinicians to directly communicate with patients.

SEFT/MedSEFT is used by NIH ICOs to facilitate collaboration and share data with internal and external stakeholders, in a secure approved on-prem environment. Users can collaborate on documents via a shared workspace or simply upload files or initiate messages to external stakeholders.

The type of data and information that SEFT will store or maintain, includes:
Name
Email
Phone
DOB
Mailing address
Employment status
Driver's license number
Mother's maiden name
Education records
Medical Notes
Certificates
Military status
Legal documents
Taxpayer ID
Passport number
Device identifiers
Photographic identifiers
Demographic data
Vehicle identifiers including license plate information
Employee Records
Training records

Insurance Information
Executable files with extensions of .exe, .jar, .dmg, .pkg, .msi, and .war
Social Security Numbers (SSN), including last 4 digits
Credit Card Numbers (CCNs)
Medical/patient information, Medical Record Number (MRN)
Grant or contract information
Sensitive network and system data/information.
System vulnerability and compliance information
NIH third-party proprietary information
Sensitive network and system data/information
System vulnerability and compliance information
IP Address

PII and sensitive PII that is collected, maintained and/or stored outside the scope of this PIA is the responsibility of the NIH ICO and a separate PIA must be prepared. Furthermore, sharing PII is subject to the Privacy Act and should only be disclosed in accordance with the law. Data may become PII or Sensitive PII due to context of use.

CIT has implemented the following security safeguards:
NIH Firewall protection
MFA requiring more than one method to verify the user's identity.
Files uploaded and downloaded via the website are transmitted with TLS encryption. Uploaded files are encrypted at-rest using AES 256-bit encryption. This software conforms to FIPS 140-2 “Security Requirements for Cryptographic Modules”.

User Access
Users log in to this system using the NIH IAM Services which maintains its own unique PIA on record, including all legal authorities documented.

For individuals internal to NIH, such as business partners, collaborators, and researchers; the system uses NIH Federated Services, a centralized authentication hub for web-based applications at NIH, instead of storing a user’s login credentials.

External users can only access and reply to emails sent to them by a NIH or HRSA user. External users cannot initiate new file transfers from SEFT. External users must contact the NIH IT Service Desk to set up an account in order to retrieve and read SEFT messages.

SEFT and MedSEFT are operated and managed by CIT UCC.

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
Encrypted messages and files, Training records, license plate information
IP address, Demographic data, Insurance Information, Employee Records
NIH third-party proprietary information, Sensitive network and system data/information , System vulnerability and compliance information
Credit Card Numbers (CCNs), Medical/patient information, Grant and/or contract information

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
Patients

How many individuals' PII is in the system?

50,000-99,999

For what primary purpose is the PII used?

To securely transmit and share (encrypted) messages and files.

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

N/A

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

5 U.S.C. 301, 302, 1302, 2951, 4118, 4308, 4506, 7501, 7511, 7521; 44 U.S.C. 3101 and 3102; Executive Order 10561

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.

09-90-0024 - Financial Transactions of HHS Accounting and

OPM/Govt-1 - General Purpose Records

09-25-0216 - Administration: NIH Electronic Directory

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

Online

Government Sources

Within the OPDIV

Other Federal Entities

Non-Government Sources

Public

Private Sector

Identify the OMB information collection approval number and expiration date

An Office of Management and Budget (OMB) collection approval number is not required as SEFT is not soliciting information.

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.

N/A

Describe the procedures for accounting for disclosures.

User and system audit logs are in place when information is accessed.

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

Users voluntarily provide name, email and password in order to use SEFT/MedSEFT.

SEFT/MedSEFT links to the NIH Web Policies and Notices page.

PII contained in files are pulled from other systems that maintain their own unique PIA. An example of a source system would be Microsoft 365, where users frequently collaborate on documents or store files within the NIH.

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.

Inclusion is voluntary. If a user doesn't want to provide PII to encrypt emails, they don't have use to the SEFT/MedSEFT application.

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

Registered NIH users are notified via email if there is a major change to the system.

External users are not notified. External users can only access and reply to emails sent to them, by a NIH or HRSA user. External users cannot initiate a file transfer from SEFTMedSEFT.

The login page/ front page of SEFT/MedSEFT Website will include supplementary notification of major system changes including updates or change in terms of service should they occur.

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.

Users may contact the SEFT/MedSEFT administrators, their Institute/Center/Office (ICO) privacy coordinator or the NIH Senior Official for Privacy (Privacy@mail.nih.gov) for opportunities for redress.

SEFT/MedSEFT would follow the Incident Response Plan in the case of concerns of data leaks/breaches/etc.

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

Periodic audits are conducted to ensure the data's integrity, availability, accuracy and relevancy.

Files, attachments and messages are deleted after 30 days. De-identified metadata may be held indefinitely.

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 PII is assigned to personnel based upon current job responsibilities. The system uses specific login information to assign permissions/user roles which is considered PII.

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.

Determinations are made based on role based access controls and least privilege. User rights are provisioned based on controls within the system, allowing users only access to the minimum amount of PII necessary to perform their job.

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.

According to NIH policy, all personnel who manage or operate NIH applications must successfully complete annual security awareness training. 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).

Administrators and Privileged Users require additional training specific to their roles and

responsibilities.

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.

Records are retained and disposed of under the authority of the NIH Records Retention Schedule.

Item 10-101 - Administrative records maintained in any agency office.
Administrative records maintained in any agency office. Records accumulated by individual offices that relate to routine day-to-day administration and management of the office rather than the mission-specific activities for which the office exists, excluding records scheduled elsewhere in the GRS such as timekeeping and procurement.
Disposition: Destroy when business use ceases. DAA-GRS-2016-0016-0001

Item 07-201: Systems and data security records.
These are records related to maintaining the security of information technology (IT) systems and data. Records outline official procedures for securing and maintaining IT infrastructure and relate to the specific
systems for which they were written. This series also includes analysis of security policies, processes, and guidelines, as well as system risk management and vulnerability analyses.
Disposition: Destroy 1 year(s) after system is superseded by a new iteration or when no longer needed for agency/IT administrative purposes to ensure a continuity of security controls throughout the life of the system. DAA-GRS-2013-0006-0001

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

Physical Controls: The IT hardware used to host protected information is located in a secured datacenter facility. The facility is only open to authorized personnel whose access is monitored by locking doors with badge readers for both ingress and egress. The facility is under 24-hour surveillance by facilities security for security and environmental hazards.

Technical Controls: Access to the system is controlled by NIH log-in which authenticates the user prior to granting access. Two factor authentication must be used for access. Access controls lists and event logs are maintained and monitored to detect unauthorized, suspicious or malicious activity. Access lists are restricted to approved IT technical personnel. File integrity and auditing software are employed and system are behind the NIH network firewall.

Administrative Controls: All technical personnel who access IT systems which contain protected information have met background investigation criteria for Public Trust positions. Personnel accessing these systems use privileged and separate accounts for administrative access to systems.

Identify the publicly-available URL:

https://secureemail.nih.gov/bds/Main.do

Note: web address is a hyperlink.

Does the website have a posted privacy notice?

Yes

Is the privacy policy available in a machine-readable format?

Yes

Does the website use web measurement and customization technology?

Yes

Select the type of website measurement and customization technologies is in use and if it is used to collect PII.

Does the website have any information or pages directed at children uner the age of thirteen?

No

Does the website contain links to non- federal government websites external to HHS?

No

Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?

null