US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

08/26/2025

OPDIV:

NIH

Name:

NIH InfoSec Archer

PIA Unique Identifier:

P-5815957-202864

The subject of this PIA is which of the following?

Minor Application (child)

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?

No

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.

Archer Security Governance, Risk, and Compliance (SGRC) is a multipurpose platform that allows NIH to assess Federal Information Security Management Act (FISMA), Privacy Act, and Office of Management and Budget (OMB) Circular A 130 (OMB A130) compliance and authorize information systems across the NIH enterprise to ensure these systems are operating at an acceptable level of risk.

Archer provides NIH, and its Institutes, Centers, and Offices (ICOs), the capability to define authorization boundaries, allocate and assess security and privacy controls, assemble authorization packages, make informed authorization decisions, and determine whether each information system stays within acceptable risk parameters.

NIH uses the Archer Security Operations (SecOps) module for security incident reporting to HHS and the Computer Security Incident Response Center (CSIRC). The SecOps Module performs the following operations:

Provides the entirety of NIH and ICOs a hub for incident reporting, response, and tracking.

Incident Ticket creation and tracking for security issues.

Document incident analysis.

Incident mitigation, including incident notification, change requests, and incident notification.

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

Personally identifiable information (PII) collected, maintained and/or shared by Archer includes:

Legal Name
Government furnished equipment (GFE) device identification (ID)

Incidental PII (due to a breach) includes:
E-Mail address
Phone Number
NIH physical address
NIH employee (ID)
HHS Badge Number
Company name (if direct contractor)

Incident analysis information covered is related to the user who is affected by an incident or the user by whom the incident occurred.

Notifications are sent to the Information System Security Officer (ISSO) and Cyber-Security Operations (CSO) team via email auto-generated by the Incident Response Team (IRT) Portal.

Those requiring access to this system log in using the NIH Identity, Credential, and Access Management (IAM) Services which maintains its own unique privacy impact assessment (PIA) on record, with 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 collects unique user credentials and stores them in an encrypted format. The IAM Service is 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.

Archer Security Governance, Risk, and Compliance (SGRC) is a multipurpose platform that allows NIH to assess Federal Information Security Management Act (FISMA), Privacy Act, and Office of Management and Budget (OMB) Circular A 130 (OMB A130) compliance and authorize information systems across the NIH enterprise to ensure these systems are operating at an acceptable level of risk.

Archer provides NIH, and its Institutes, Centers, and Offices (ICOs), the capability to define authorization boundaries, allocate and assess security and privacy controls, assemble authorization packages, make informed authorization decisions, and determine whether each information system stays within acceptable risk parameters.

NIH uses the Archer Security Operations (SecOps) module for security incident reporting to HHS and the Computer Security Incident Response Center (CSIRC). The SecOps Module performs the following operations:

Provides the entirety of NIH and ICOs a hub for incident reporting, response, and tracking.

Incident Ticket creation and tracking for security issues.

Document incident analysis.

Incident mitigation, including incident notification, change requests, and incident notification.

Personally identifiable information (PII) collected, maintained and/or shared by Archer includes:

Legal Name
Government furnished equipment (GFE) device identification (ID)

Incidental PII (due to a breach) includes:
E-Mail address
Phone Number
NIH physical address
NIH employee (ID)
HHS Badge Number
Company name (if direct contractor)

Incident analysis information covered is related to the user who is affected by an incident or the user by whom the incident occurred.

Notifications are sent to the Information System Security Officer (ISSO) and Cyber-Security Operations (CSO) team via email auto-generated by the Incident Response Team (IRT) Portal.

Those requiring access to this system log in using the NIH Identity, Credential, and Access Management (IAM) Services which maintains its own unique privacy impact assessment (PIA) on record, with 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 collects unique user credentials and stores them in an encrypted format. The IAM Service is 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.

Name
E-Mail Address
Phone Numbers
NIH physical address, NIH employee ID, Badge Number
Company name, GFE Device ID

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

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

How many individuals' PII is in the system?

10,000-49,999

For what primary purpose is the PII used?

Data is used for incident identification.

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

None

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

The Computer Security Act, Pub. L.100-235; and FISMA, 44 U.S.C. § 3541, et seq.

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.

09-25-0216 Administration: NIH Electronic Directory

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Email

Online

Non-applicable

Government Sources

Within OpDiv

Non-Governmental Sources

Private Sector

Identify the OMB information collection approval number and expiration date

Is the PII shared with other organizations?

No

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

NIH Rules of Behavior and warning banners are displayed on NIH logon screens to access NIH systems. Users are required to read and accept these notices to obtain access. Additionally, consent is given when an individual enters into a business relationship with 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.

The PII is automatically collected in relation to the incident. Individuals cannot opt out.

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

Notification and consent is part of the on-boarding process. It is given when an individual enters into a business relationship with NIH.

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 can contact the NIH IT Service Desk or NIH Privacy Office at: Privacy@mail.nih.gov

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 CSO and CSIRC teams perform periodic reviews of the collected. incident data

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.

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.

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.

Archer follows NIH policy to employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

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 and privacy 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 of the system are provided with system training via Microsoft (MS) Teams and training documentation.

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.

07-203, System access records. Destroy when business use ceases (DAA-GRS-2013-0006-0003).

07-107, Information technology oversight and compliance records. Destroy 5 years after the project/activity/ transaction is completed or superseded, but longer retention is authorized if required for business use (DAA GRS-2013-0005-0010).

07-202, Computer security incident handling, reporting and follow-up records. Destroy 3 year(s) after all necessary follow-up actions have been completed, but longer retention is authorized if required

for business use (DAA-GRS-2013-0006-0002).

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

Administrative Controls: Include system security and contingency plan. Files are backed up regularly and stored offsite. Contract clauses ensure adherence to privacy provisions and practices, least privilege through role-based access, and policies for retention and destruction of PII.

Technical Controls: Access to the system is controlled by NIH log-in which authenticates the user prior to granting access. Access level and permissions are controlled by the system and based on user, role, organizational unit, and status of the report. All servers have been configured to remove all unused applications and system files and all local account access except when necessary to manage the system and maintain integrity of data.

Physical Controls: Archer is hosted in the CIT Amazon Web Services (AWS) environment. Physical controls are inherited from AWS.