US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

03/11/2025

OPDIV:

NIH

Name:

1099 Pro

PIA Unique Identifier:

P-3678315-157653

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?

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.

N/A

Describe the purpose of the system.

1099Pro is used to create Internal Revenue System (IRS) 1099 forms for eligible entities and persons who received miscellaneous payments from the National Institutes of Health (NIH) in the calendar year.

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

1099Pro collects data related to 1099 forms. Personally Identifiable Information (PII) that is collected includes: Name, Social Security Number (SSN), email address, tax payer identification (ID), mailing address, State/Payer's state number, and applicable account numbers. Additional non-PII data could include: rents, royalties, health care payments, attorney fees paid, and tax withholding information.

The system uses specific login information to assign permissions/user roles which is considered PII. However, this is done using the 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. The IAM Services collect unique user names and passwords (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.

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

1099Pro is used to create IRS 1099 forms for eligible entities and persons who received miscellaneous payments from NIH in the calendar year.

1099Pro collects data related to 1099 forms. PII that is collected includes: Name, SSN, email address, tax payer ID, mailing address, State/Payer's state number, and applicable account numbers. Additional non-PII data could include: rents, royalties, health care payments, attorney fees paid, and tax withholding information.

The system uses specific login information to assign permissions/user roles which is considered PII. However, this is done using the NIH IAM Services which maintains its own 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 names and passwords (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.

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
Name
E-Mail Address
Mailing Address
Taxpayer ID
Account Numbers
State/Payer's State number
Financial information

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

Employees
Public Citizens
Vendor/Suppliers/Contractors
Patients

How many individuals' PII is in the system?

10,000-49,999

For what primary purpose is the PII used?

The primary purpose of the collected PII is to create 1099 tax forms for Payees that receive money from NIH.

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.

5 U.S.C. 301 and 302, U.S.C. 3322 and 31 CFR 210 authorize the collection of the payment information, 44 U.S.C. 3101
and 310231

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.

09-25-0217, NIH Business System (NBS)

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains
Online
Government Sources
Within the DOC
Other Federal Entities
Non-Governmental Sources
Public

Identify the OMB information collection approval number and expiration date

1545-0115 Expiration: 07/31/2026

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.

There are currently no agreements in place. Reporting to the IRS is a federal requirement for tax purposes.

Describe the procedures for accounting for disclosures.

Information is not disclosed other than to the individual who the PII belongs to and to the IRS. Audit trails exists to track disclosures.

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

Individuals are notified verbally or electronically about the PII being collected for issuing federal payment and tax reporting purposes during the collection of information.

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.

Individuals may opt-out of the collection and use of their PII by not providing their information. However, the collection of PII is a requirement to process Federal payments for tax reporting purposes. Failure to give this information will lead to the individual not being able to receive payment from NIH.

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

Individuals can contact the NIH Office of Financial Management (OFM) to update their PII via phone or email. The PII data is not disclosed or updated without the verbal or electronic consent from the individuals whose PII is updated. The system does not have the capability to notify the users of the changes to disclosure or data uses as this application is a standalone application used for the sole purpose for filing the tax forms to IRS. Any Changes to the data use or disclosure are driven by IRS Mandates, OFM and the program offices will inform the payees about the update to these changes as when required.

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.

If an individual believes that their PII has been inappropriately obtained, used, disclosed or that the PII is inaccurate, that individual may contact OFM.

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

OFM conducts periodic review of PII data to ensure the integrity, availability, accuracy and relevancy of the data. The PII data is removed as per the Record Retention scheduled accordingly.

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.

The procedure requires all changes be verified by the supervisor on weekly basis. System users access to PII is approved based on their technical/functional role in administering, developing, and supporting the daily job functions of the system.

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).

There is specific role based training to ensure the importance of securing PII.

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.

Item Number: 05-102: Financial Transaction Records Related to Procuring Goods and Services, Paying Bills, Collecting Debts, and Accounting. Official Record Held in the Office of Record.

Description: Many records included in this item are maintained by accountable officers to account for the availability and status of public funds, and are retained to enable GAO, Office of Inspector General, or other authority audit.
Financial transaction records include those created in the course of procuring goods and services, paying bills, collecting debts, and accounting for all finance activity, per the following definitions.
Disposition Instruction: Destroy 6 years after final payment or cancellation, but longer retention is authorized if required for business use. The following Controlled Unclassified Information (CUI) applies to this schedule.
Disposition Authority Agency (DAA): DAA-GRS-2013-0003-0001

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 data center facility. The facility is only open to authorized personnel whose access is monitored by locking doors with badge readers for both ingress and egress. Each discrete ingress and egress event is logged. The facility is under 24-hour surveillance by facilities security for security and environmental hazards.

Technical Controls: IT hardware and software is segregated from default commodity public networks to prevent unauthorized or malicious 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. Two factor authentication must be used for access. File integrity and auditing software are employed on hardware.

Administrative Controls: All technical personnel who access IT
systems which contain protected information have met background investigation criteria for Public Trust positions. All personnel have taken mandatory security and privacy training classes and annual refreshers. Administrative personnel accessing these systems use privileged and separate accounts for administrative access.