US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

10/26/2016

OPDIV:

OIG

Name:

Snap Survey

PIA Unique Identifier:

P-6617993-593503

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?

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.

SNAP Survey is a software to build data collection instruments (web surveys).

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

As a part of oversight and review of HHS programs, the Office of Evaluation and Inspections (OEI) will collect information from respondents and review their responses. This information will be analyzed and reported out in published reports. Such information may include name, email address, phone numbers, mailing address, medical notes, medical records information, medical claim identification number, Medicare and/or Medicaid ID, medical provider identifiers, application materials, tax ID, legal documents, Provider NPI, payment processes, other official documents and user credentials and passwords

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

On behalf of the OEI SNAP Survey collects information from respondents as a part of our oversight and review of HHS programs. The information the OEI regional offices collect, maintain or disseminate varies based on the type of study being conducted. The information may include general questions about the types of services Medicare or Medicaid providers bill for, estimated number of services performed by a particular provider, groups of providers, or categories of providers, issues in provision of service(s), payment processes, summary of procedures performed, etc. OEI will use the information gathered to report any findings, violations, or issues in a written report. Information that might be collected in an instrument includes name, email address, mailing address, medical records information, medical claim identification number, Medicare and/or Medicaid ID, medical provider identifiers, application materials and other official documents and user credentials and passwords for system management.

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

Mailing Address

Phone Numbers

Medical Notes

Financial Accounts Info

Legal Documents

Taxpayer ID

Claim IDs

Medicare or Medicaid IDs

Provider NPI

User credentials

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

Employees

Business Partner/Contacts (Federal/state/local agencies)

Vendor/Suppliers/Contractors

Patients

How many individuals' PII is in the system?

1,000,000 or more

For what primary purpose is the PII used?

PII is used for evaluations involving oversight of HHS programs.

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

No secondary uses.

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

Inspector General Act of 1978

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

No

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Online

Government Sources

Within OpDiv

Non-Governmental Sources

Public

Private Sector

Identify the OMB information collection approval number and expiration date

None

Is the PII shared with other organizations?

Yes

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

Within HHS

Oversight of HHS programs.

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

N/A

Describe the procedures for accounting for disclosures.

Individual staff maintain a spreadsheet with logging and tracking of all computer-based data files that contain sensitive information. Staff are required to update log spreadsheet every six months and log any transfer of sensitive information inside and outside of the OIG.

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 either notified in cover letters to the survey and/or in the introduction to the survey itself about the purpose of the collection and how the information will be used. Users who provide PII in the form of credentials to access the system are not provided explicit notice that their personal information is collected and securely maintained by the system. These HHS OIG users are considered to consent to this collection as a prerequisite for system access.

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.

In many surveys providing PII is not required to complete the survey. If respondents have questions or concerns, contact information for the evaluation team is provided to all respondents. If they do not want to provide information, the evaluation team along with the Office of Counsel for the Inspector General (OCIG) determine what information is required to be provided. HHS OIG users are not able to opt-out as the unique user credentials are necessary to allow for system management and non-repudiation.

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

It is not the purpose of this survey system to collect PII. However, if PII is collected, each regional office will include a statement on how the information will be used or shared. OEI regional office has the option of selecting whether the format of notice of consent will be written or electronic. The method of communicating the notice of consent may be either via mail or email.

By participating in the survey after receiving the notice, individuals are considered to have consented to the collection of the information they provide. HHS OIG users are not able to opt-out as the unique user credentials are necessary to allow for system management and non-repudiation.

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 contact the evaluation team point of contact with any questions or concerns. These issues will be escalated as appropriate to the OEI POC in charge of the collection and/or HHS OIG Office of Counsel. The same process is in place for HHS OIG users with questions or concerns.

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

PII reviews are included in the annual security and privacy controls assessments. This incorporates the NIST 800-53r4 Appendix J Privacy Controls and provides an opportunity to assess the need for all of the PII in the system. Should PII elements be deemed unnecessary the appropriate steps would be taken in conjunction with the system administrator to remove those elements.

Records are maintained in a restricted area and accessed only by Department personnel. Access within OIG is strictly limited to authorized staff members. All employees are given instructions on the sensitivity of such files and the restrictions on disclosure. Access within HHS is strictly limited to employees on a need-to-know basis. All main frame computer files and printed listings are safeguarded in accordance with the provisions of the National Institute of Standards and Technology Federal Information Processing Standards 41 and 31, and the HHS Information Resources Management Manual, Part 6, "ADP Systems Security."

User credentials are unique and provide a mechanism through which all edits, modifications or deletions of data, including PII, in the system can be tracked. Audit logs are used to identify which users log in and which commands are executed. All staff are required to maintain a log of all computer-based data files that contain sensitive information - including PII - and update it every six months.

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

Users:

To execute the OEI tasks identified for each study.

Administrators:

To maintain system.

Contractors:

Direct contractors as needed to maintain and update the system.

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

The information is maintained on a centrally managed OIG computer system. Access is restricted by physical and computer-based access controls. Access is strictly limited to authorized OIG staff members via a two level authentication process. Users must be initially authenticated as valid OIG staff and are then authenticated to the Audit & Evaluation System by an independent second level authentication system. Users are granted system access only after demonstrating a valid business purpose and are given access in accordance with principles of least privilege. All computer files and printed listings are safeguarded in accordance with Federal and departmental guidelines. Access to information technology assets is limited to individuals possessing the appropriate badging and access permissions (granted with a demonstrated valid business need.)

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.

Stored documents in the report work papers have indicators on documents that contain PII.

Staff are instructed to access documents identified as PII only if it is necessary. Access to digital information is limited to those with a demonstrated need to know based on a bona fide business need.

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.

Annual Departmental and OIG training to ensure staff is aware their responsibilities for protecting the information being collected and maintained. Additionally, refresher training on a regular basis for current staff and initially at new employee training.

OEI has also issued guidance to all personnel concerning the protection of sensitive information and procedures for reporting the loss of personally identifiable information and logging and tracking all computer-based data files that contain sensitive information.

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

OIG is planning role-based training for all personnel who routinely access sensitive information. A reminder of the responsibility for recording sensitive information is also covered in OEI's SNAP Survey user 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.

SNAP Survey follows the policies and guidelines set forth in the HHS OIG guidelines for retention and destruction of sensitive information.

OIG DAA-0468-2013-0012: Transfer to Federal Records Center two years after cutoff (end of fiscal year in which evaluation is closed) and destroy 5 years after cutoff.

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

The information is maintained on a centrally-managed OIG computer system. Access is restricted by physical and computer-based access controls. The IT infrastructure is located within secured buildings. Appropriate physical security controls have been implemented at all locations - these may include access badges, security guards, Closed Circuit TV, and/or cipher locks. Logical controls which minimize the possibility of unauthorized access, use, or dissemination of the data in the system are in place. Access is strictly limited to authorized OIG staff members via a two level authentication process. Users must be initially authenticated as valid OIG staff and are then authenticated to the Audit & Evaluation System by an independent second level authentication system.

All computer files and printed listings are safeguarded in accordance with Federal and departmental guidelines.

SNAP Survey files are backed up regularly and stored offsite.

Identify the publicly-available URL:

https://nihoigsurvey.cit.nih.gov/snapwebhost/

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?

No

Does the website have any information or pages directed at children under 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