

US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

08/31/2016

OPDIV:

HRSA

Name:

Insure Kids Now

PIA Unique Identifier:

P-7455442-896736

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?

Yes

Identify the operator.

Agency

Is this a new or existing system?

New

Does the system have Security Authorization (SA)?

No

Indicate the following reason(s) for updating this PIA.**Describe the purpose of the system.**

The purpose of the IKN system is to collect dental provider data from states and their authorized representatives and publish it through a publicly available website so families can find a dentist for their children who accepts health plans managed under Medicaid and Children Health Insurance Program (CHIP).

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

The system collects and maintains two types of information: 1) dental provider and health program details intended to be published in a publicly available site. The individual fields collected for publication are outlined in the IKN Technical Guidance document available at: <https://ikndata.insurekidsnow.gov/WebExternal/files/Insure%20Kids%20Now%20Technical%20Guidance.docx>. It includes information such as the name of the health insurance program, the name of dental providers, group practices, and/or facilities, the address where services are provided, and the phone number where a member of the public could call to make an appointment with the listed provider. The data published in the IKN dental provider locator tool does not contain any PII.

2) The second category of information is information collected from state administrative users (users who work directly for a state government and their representative (contractor organizations authorized by the state to upload data on their behalf) that is needed to administer the website used to collect the provider data. This includes the name, email address, phone number, and mailing address of the state administrative user or contractor. This information is collected so that the federal agency representatives (CMS & HRSA) and the system administrators have access to contact information for system users to advise them of upcoming system changes, to distribute communications regarding webinars or materials of interest to them, and to provide technical assistance to the individuals using the system. The data needed to administer the website that is used to collect the provider data is not accessible to anyone besides system administrators.

Information provided by public citizens accessing the publicly available dental locator tool are provided as search criteria used to filter the results to give them information most relevant to their needs. Search criteria may include the following: requests to filter the data by location (address, ZIP code, city name, state name), name of a health insurance plan, whether a provider accepts new patients, provider specialty, and languages spoken by the provider.

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

The Insure Kids Now system has two primary components: the publicly available locator tool and the IKN Data Management website. State administrative users and their authorized representatives use the IKN Data Management website to upload files containing dental provider details and to edit health plan information. That information is then published through the Insure Kids Now public website so families can use the IKN locator tool to find dentists for their children.

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

None of the information above is provided by public citizens on the publicly available website.

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

Public Citizens

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

Vendor/Suppliers/Contractors

No PII is entered by or about public citizens on the publicly available website.

How many individuals' PII is in the system?

100-499

For what primary purpose is the PII used?

The primary purpose is to provide a means for the IKN federal team and contractor staff to contact users of the IKN Data Management Site regarding communication required to maintain normal business operations.

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.

Section 501(f) of the Children's Health Insurance Program (CHIP) Reauthorization Act of 2009 required the Department of Health and Human Services (HHS) to post on its Insure Kids Now (IKN) website a current and accurate list of dentists and providers within each State that provides dental services to children under Medicaid and CHIP programs. The Centers for Medicare and Medicaid Services (CMS) and the Health Resources and Services Administration (HRSA) partnered to meet this requirement, and developed a file submission format, protocol, and basic validation process that the various State CHIP and Medicaid offices use to submit the data. No PII is entered or published on the publicly available website.

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

No

Identify the sources of PII in the system.

Online

Government Sources

State/Local/Tribal

Identify the OMB information collection approval number and expiration date

0938-1065; Expiration date: 2/28/2018

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.

The online form used to create accounts has fields identified which are part of the registration process. On the login page, there is a warning message advising the user that they're accessing a government system and are advised of general policies of use. There is also a link to the HHS privacy policy at the bottom of the login page.

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.

IKN Data Management System collects the following elements: Name, address, email address, and phone number. Currently there is no option to opt out of providing these data elements because at the time the system was developed, there was a request to collect this information to provide a means to communicate with system users as a normal part of doing business. In the future, the IKN team is planning to deprecate the requirement to provide phone numbers and address information. Names and email addresses will still be needed for the purposes of maintaining normal business operations. The only way to "opt out" of providing this information is to elect not to register as a system user, which would prevent the individual from accessing the system entirely.

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

In the event of major system changes, users are contacted by emails sent out by staff managing the IKN technical help mailbox.

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 a user has a concern about their PII, they may contact the IKN technical help mailbox or may contact an HHS Privacy Official as referenced in the HHS Privacy Policy Notice posted on the site.

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 collected is maintained solely for the purpose of contacting State Administrators or contractors acting on their behalf. State Administrators and contractors working for the State Administrators authorized to upload data on their behalf do not have access to see or edit any PII. If a user no longer has the need to upload data on behalf of the State Administrator, then their accounts will be disabled at the request of the State Administrators.

The IKN federal team and system administrators have standard bi-weekly meeting to discuss system status, enhancements, change requests, reviews of PII and user account are monthly. There is an automated system monitoring function to check the availability of the database in which the data are stored at configurable intervals. If an issue is detected, the monitoring tool sends an automated alert to system administrators to take appropriate action.

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

Administrators:

PII not available through the IKN website; only available as an extract from the database, which has controlled access. System administrators have access to manage access permissions and to make changes to the data structure and front facing applications as needed.

Developers:

PII not available through the IKN website; only available as an extract from the database, which has controlled access. Developers need to be able to access the system to make changes to the data structure and front facing applications as needed.

Contractors:

PII not available through the IKN website; only available as an extract from the database, which has controlled access. Contractors serve as system administrators and developers and access the system for the reasons described above.

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

The access is controlled by Active Directory groups based on role. The roles are determined by management staff which is based on need. All users are limited to the functions and information which is essential to their job functions.

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.

Databases containing the PII have security access controls in place to limit access to the content. Team members with access to production data may access all data in 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.

HRSA requires federal staff and contract personnel to take mandatory trainings relating to security and privacy issues on an annual basis.

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

None.

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.

HRSA is working with National Archives and Records Administration (NARA) to develop a system records schedule and pending approval and finalization of an appropriate disposition schedule with NARA, the records will be retained permanently until scheduled.

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

PII stored elsewhere in the system is secured through database login restrictions; server login restrictions; and HRSA network login restrictions.

Access to this information is further restricted by user role. Policies are in place to review / test the security controls that are in place to protect the PII data. All users are trained annually on how to protect PII data and what steps to take in case of data breaches. Users accessing this data must use 2 factor authentication to access the data. There are controls in place to automatically log users off if theres a period of inactivity.

Physical controls include the need for an authorized badge ID to access a locked suite and a separate badge with authorized user credentials to access production data on the system. The servers are secured in a data center which is restricted to authorized personnel only and is monitored by video surveillance.

Identify the publicly-available URL:

<https://ikndata.insurekidsnow.gov/WebExternal/Login.aspx>

(Administrative website; PII collected as a means of contacting system users).

<http://insurekidsnow.gov/>

(Publicly available provider data; no PII available). The IKN Data Management system pushes provider data to an application embedded within an iframe on <http://insurekidsnow.gov/>, a website maintained by CMS (not within the system boundary). If there are cookies on that website, this system has no control over that.

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.

Session Cookies that do not collect PII.

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?

Yes

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

No