US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

08/16/2016

OPDIV:

AHRQ

Name:

HCUP Central Distributor Ordering Web site

PIA Unique Identifier:

P-8598756-235086

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.

Contractor

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 Healthcare Cost and Utilization Project, Central Distributor Ordering Website System (HCUP-CDOW) is an online system that makes restricted data products and tools available for qualified applicants to purchase for scientific research and public health use. Applicants may be researchers, patients, consumers, practitioners, providers, policy makers, or educators. The HCUP data products consist of annual files containing anonymous information from hospital discharge records for inpatient care and certain components of outpatient care. The HCUP software tools enhance the use of the data. The online system supports AHRQ's mission of promoting improvements in health care quality. The Web site consists of:

A data product catalog for users to view the products available. Public users may browse the product catalog, but only users who have completed HCUP Data Use Agreement training and registered as customers may complete applications for the purchase of HCUP data products.

Information about the application process, including documents that need to be supplied, either digitally or hard copy, as part of the application and fulfillment process.

Application and order processing steps in which the Web site gathers applicant contact information and project detail that is needed to fulfill the request. An applicant can save an incomplete application and return to complete it at a later date.

HCUP data products at the nationwide level are delivered via secure download after the ordering process is complete and payment has been received. HCUP data products at the State level are shipped to the customer on physical media.

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

HCUP CDOW is a system used to facilitate the ordering of HCUP data products and also for the fulfillment of the orders. To meet these objectives, the System collects information from those purchasing the products and the System also stores the data products themselves which are encrypted HCUP Nationwide data products.

In order to create, save, and submit an online application for data file purchases, the user must register for an account. The system collects and stores the contact information elements listed below. Most applicants are affiliated with research organizations and therefore supply business or institution address/phone rather than personal information: name, mailing/shipping address, phone number, fax number, email address, username and password, organization name, organization type (Government, Non-Profit, For-Profit, etc.). For each order/application the system also collects: description of project and how HCUP data will be used; current College/University attending billing name, address (if different from shipping), and phone; indication of student status; the title and number of AHRQ project grant, if applicable; payment authorization code, if applicable; list of HCUP data files on order; and, data use agreement(s) (DUA) applicable to the data file(s) selected for purchase.

DUAs for applicants are stored in PDF format and contains the applicant's name, mailing address, phone number, and email address.

The data products provided by the system contain hospital discharge data provided by the HCUP data provider organizations.

For site administrators, a username and password are created and stored.

The CDOW refers users to the HCUP-US Web site for all information pertaining to the databases and data sources. The HCUP CDOW is accessible only by navigating through the HCUP-US Web site, and exists solely to support the HCUP project. A separate Privacy Impact Assessment is maintained for the HCUP-US Web site.

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

The Web site maintains a database catalog listing the current HCUP data products that are available to order. The Web site uses e-commerce technology to allow the applicant to add selected products to a shopping cart. The Web site presents payment choices to the applicant including mailing a check, purchase order, wire transfer, or making immediate payment using a credit card. Credit card purchases are handled securely using a third party PCI-compliant payment gateway. Credit card information is never stored; the authorization code is stored for 30 days.

No applicant information is shared or used for any purpose other than A) managing order fulfillment and B) potential future follow-up in the event of a DUA violation.

Applicants have the option to submit applications in hard copy format. Hard copy applications are entered into the system upon receipt by operations staff, unless the applicant explicitly opted out of online storage of PII.

HCUP data file products are divided into two broad groups: State data products and nationwide data products. State data products are not stored on the Web site; they are stored on a standalone system, which cannot be accessed from any Web site or network, and are provided to customers through a separate medium. Nationwide data products are stored in encrypted, compressed format on a separate server with an encrypted hard drive. The e-commerce technology provides the secure digital download of nationwide data products to qualified, verified purchasers.

The CDOW system does not collect or maintain the de-identified information which is contained in the HCUP data products. The HCUP-CDOW System consists of multiple servers each serving a different function including Web server, database server, and file storage server working together as a seamless system to the end-user. Only the Web server is accessible to external users and hosts the interface that customers will interact with including the Web site. The database server stores information necessary to facilitate online transactions such as customer information and the file server stores the data products available for download.

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

Legal Documents

Fax Number

Organization Name

User credentials (username and password)

Billing Address and Phone

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

Employees

Public Citizens

No PII is collected on any type of entity other than public citizens who register to purchase database products.

How many individuals' PII is in the system?

10,000-49,999

For what primary purpose is the PII used?

PII is used for contact and billing information to fulfill the request to purchase HCUP data.
For system users / administrators PII is used for identification, authentication, and password reset.

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

Potential future follow-up to contact the user in the event of a DUA violation.

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

Section 913 and 306 of the Public Health Service (PHS) Act (42 U.S.C. § 299b-2 and 242k(b)). Sections 924(c) and 308(d) of the PHS Act (42 U.S.C. 299c-3(c) and 242m(d)) provide authority for protecting restrictions on identifiable information about individuals. Privacy Act of 1974; E-Government Act of 2002; OMB M-03-22, OMB 07-16, OMB M-10-23, 42 U.S.C. 299-299a, 42 U.S.C. 299c-2.

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.

09-90-1401 Recs. About Restricted Dataset Req.

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

Hardcopy

Email

Online

Government Sources

Within OpDiv

Non-Governmental Sources

Public

Identify the OMB information collection approval number and expiration date

0935-0206 - Expires 01/31/2019

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.

Use of the Web site system is voluntary and utilized only for the application process for data product purchase. The collection of information and its intended use is detailed in the privacy policy which is available in the footer of every page on the Web site. Users who are AHRQ employees and direct contractors are notified at the time of collection that their information will be collected in order to provision an account, prior to access to the account being granted to the user.

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.

Customers must provide their contact information to obtain HCUP data products, and there is no option for objecting to the collection and use of PII. The information is necessary for processing orders and delivery of products. The information is also necessary to document signed Data Use Agreements (DUA) and enforce restrictions in the event of a violation of the DUA. Users who are AHRQ employees and direct contractors cannot opt out of the collection of user credentials, as the credentials are necessary to provision and verify account access for the system.

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

No changes are anticipated that would change how the system stores, protects, or discloses PII. If a change ever were to require notification, the system provides for email contact mechanisms. A relatively small number of customers submit applications hard copy, and those individuals would be contacted via phone or physical mailing if no email address was provided with the hard copy application. Users who are AHRQ employees and direct contractors are directly involved in system changes, as they perform system administration and development roles. As such, notification is not necessary for these users.

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 AHRQ via email/phone. The system allows users to correct their own inaccurate PII online, or may request that AHRQ operations staff handle it.

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

Reviews of the system are conducted annually as part of the annual security assessment to ensure integrity, availability, and relevancy according to the System Security Plan. The PII are only needed to fulfill the order associated with each application and will be retained for historical reference in the event of a DUA violation.

Customers are responsible for entering and updating their own information, e.g., address changes, but may contact the operations staff for assistance with accuracy if needed. Users who are AHRQ employees and direct contractors must use accurate information to log into their account for system access. There is no process in place to verify the integrity, availability, or relevancy of these users' PII other than users identifying an issue with account access and working with the system owner to reset or renew system account information to log into the system.

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

Users:

Only access their own information

Administrators:

System administrators have access as needed to provide technical support

Developers:

Developers have access as needed to provide technical support

Contractors:

Truven Health Analytics and SSS staff have access to facilitate the HCUP-CDOW program.

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

System user access to the data is permitted only through authorization by the AHRQ Project Director, after completion of the required data use agreements, security and privacy awareness training, public trust background check, and database-specific security training. A database is maintained by the Project Director to track all security requirements and to record all staff-specific training.

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.

Type and amount of access to PII is linked to the type of system account granted based on the person's role as authorized by the Project Director. Standard operating system and database/application controls are used to ensure that only those persons who are authorized to access this information have account access.

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.

All HCUP project staff must take the AHRQ Information Security & Privacy Awareness Training.
HHS Role-Based Training (Managers, IT Administrators, Executives)

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

HCUP Privacy Training
HCUP Data Confidentiality & Security Training
IT Admin Information Security Training Course
NIH Security & Privacy Awareness Training
For IT Administrators: IT Admin Information Security Training Course

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.

Destruction of records is scheduled for 20 years after completion of signed agreements per National Archives and Records Administration, Disposition Authority Number DAA-0510-2013-0003-0001.

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

The system follows the National Institute of Standards and Technology system security requirements based upon the system assessment and authorization (SA&A) categorization.

Physical Control: The physical hardware is secured in a private cage with multiple layers of physical access control including but not limited to 24/7 guards, mantraps, hand scanners, and private pin codes.

Technical controls: Access to the network is secured through firewall policies, system permissions, and two-factor authentication.

Administrative controls: Access through the online portal is secured through a role-based permissions access control matrix.

Identify the publicly-available URL:

https://www.distributor.hcup-us.ahrq.gov/

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?

No

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