US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

10/06/2016

OPDIV:

AHRQ

Name:

Healthcare Cost and Utilization Project Web Services

PIA Unique Identifier:

P-5724445-706022

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?

Existing

Does the system have Security Authorization (SA)?

No

Indicate the following reason(s) for updating this PIA.

PIA Validation

Conversion

Describe in further detail any changes to the system that have occurred since the last PIA.

N/A

Describe the purpose of the system.

The system consists of two separate servers, each hosting a different application. The HCUP-US Website is an informational site that disseminates information to the public about the Healthcare Cost and Utilization Project (HCUP). There is a secure password-protected portion of HCUP-US that provides information about HCUP to AHRQ, AHRQ's primary contractor for HCUP, Truven Health Analytics, and state-level organizations that provide data for the project.

Halfreski is an intranet-based application used exclusively by AHRQ's contractor, Truven Health, to manage, administer, and support HCUP. The Halfreski site is not accessible to the public.

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

The HCUP-US Web site is designed to answer HCUP-related questions; provide detailed information on HCUP databases, tools, and products; and offer technical assistance to HCUP users. The HCUP-US Web site does not contain any protected health information (PHI) or patient or facility level health data. Most of the Web site is publicly available; the password-protected area provides information pertinent only to AHRQ, contractors, and data partners. The user's name, user ID, email, and password hashes are retained for authenticating the users on the system.

The Halfreski Intranet site is a collection of four Intranet-based applications: HCUP Automated Library (HAL), HCUP Content Manager (Alfresco), Data Elements Library (DEL) and the HCUP Wiki. These four applications serve various associated management support functions for the HCUP data processing tasks, and none of the applications contain PHI, patient or facility level data, or other sensitive data. All of the applications on this site are password protected. The user's name, user ID, email, and password hashes are retained for authenticating the users on the system.

The System maintains employee and direct contractor user IDs and passwords for system administrators and content managers.

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

The System consists of two separate servers each hosting a different application: HCUP-US (public facing) and Halfreski (internal-use only). HCUP-US does not collect any information from the public or individual users. It is a “read-only” Web site for end-users and the content is managed by a site administrator at Truven Health Analytics. All content posted to the site is approved by AHRQ for public dissemination. HCUP-US provides information about HCUP and the HCUP ressearch databases that contain data that is available for purchase. The HCUP provides for purchase a family of databases and related software tools and products developed through a Federal-State-Industry partnership and sponsored by AHRQ.

HCUP databases are derived from administrative data and contain encounter-level, clinical and nonclinical information including all-listed diagnoses and procedures, discharge status, patient demographics, and charges for all patients, regardless of payer (e.g., Medicare, Medicaid, private insurance, uninsured), beginning in 1988. These databases enable research on a broad range of health policy issues, including cost and quality of health services, medical practice patterns, access to health care programs, and outcomes of treatments at the national, State, and local market levels. The secure portion of HCUP-US provides information directed to the data providers (such as information about events and technical reports and the HCUP team (such as project deliverables and data provider relationships).

Halfreski can only be accessed by Truven Health Analytics staff because it is an Intranet site. The site is used by HCUP staff to facilitate project management and collaboration for task tracking, project deliverables, management, presentations, document templates, and project-specific procedures. The site does not contain any sensitive materials or PHI.

Both sites maintain a database of user's name, ID, email, and password hash to facilitate user authentication for employees and direct contractors.

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

Direct contractor AHRQ email, user name, and password.

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

Employees

How many individuals' PII is in the system?

100-499

For what primary purpose is the PII used?

User identification, authentication, and password reset

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

N/A

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

5 USC 301, Departmental regulations

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

No

Identify the sources of PII in the system.

Email

Government Sources

Within OpDiv

Other HHS OpDiv

State/Local/Tribal

Identify the OMB information collection approval number and expiration date

N/A

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.

No prior notice is given. Individuals are notified of the collection of PII in order to provision accounts on the system, and users are notified of when their accounts are established on the system.

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 (name and email) is generally provided by the managers and administrators organization. Individual PII is used to facilitate system access and password reset only. If the individual requires/wants access to the system, the PII is required to provision access. Individuals can request their access be revoked by contacting the system owner directly.

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

Users are contacted via email in the event that PII maintained in the system would be used for purposes other than authentication and account access.

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.

The PII (name and email) is only used for tracking and granting system access and is not used for any other purpose. Therefore, there is no process in place to resolve an individual's concerns. However, if an issue arises regarding the inappropriate use of PII, users can contact the system owner directly address these 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.

Updates of PII and system access are conducted by AHRQ staff every six months. PII is backed up and can be recovered if integrity comes into doubt or system becomes unavailable. If there is an error in the PII, the user will not be able to login to the system since they will not be able to receive their credentials. Only required information (user name and email) can be entered into the System.

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

Administrators:

Direct contractors perform as website administrators and have access to user name and email to assist users that are having trouble logging into the site.

Developers:

Direct contractors perform as application developers and have access when troubleshooting or working on feature updates.

Contractors:

Direct contractors are used for system maintenance and development.

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

Separation of duties are established by the system owner and in place along with internal security controls and procedures concerning access to the system. Direct contractors not in administrator or developer roles cannot have access to the PII.

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.

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.

AHRQ Project Director and Truven Health Analytics (direct contractor staff) must take the AHRQ security and privacy awareness training prior to being granted access to the system, and must then re-take the training on an annual basis.

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

Prior to accessing HCUP data, users must also complete the HCUP Data Use training.

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.

Records needed to enforce data use restrictions are retained for 20 years by AHRQ (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.

Administrative controls for the system include annual security and privacy training, manager approval to grant system access, detailed tracking of user access accounts, quarterly access control review, separation of duties, and established least privilege principles when govering access.

Technical controls for the system include user identification, passwords with rules enforced (complexity, expiration, history), encryption during session (SSL), detailed logging of user account activities, monthly vulnerability scans, network monitoring (IDS/IPS), and network segmentation / firewalls.

Physical controls, restricted access - key cards and biometrics, video camera surveillance, emergency power – UPS and generators for power, and inventory and tracking of information system components.

Identify the publicly-available URL:

www.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.

Persistent 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?

Yes