US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

08/31/2016

OPDIV:

AHRQ

Name:

Healthcare Cost Utilization Project

PIA Unique Identifier:

P-1490188-152852

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?

No

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 system supports two research projects for the Agency for Health Care Research and Quality: the Healthcare Cost and Utilization Project (HCUP) and the AHRQ Quality Indicators (AHRQ QI).

The key activity for this system is to create and analyze the HCUP databases. This is done by collecting hospital discharge data from State data organizations (HCUP Partners) and processing the data into a uniform format. In addition, the HCUP data are utilized to support the AHRQ Quality Indicators (QI) project.

The HCUP System is a group of servers where data and work products supporting HCUP and AHRQ QI projects are securely stored. The servers are utilized exclusively by AHRQ's contractor, Truven Health Analytics, to support both projects and meet contract deliverables.

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

HCUP databases are created by collecting administrative hospital discharge data from State data organizations. The organizations that provide data to the HCUP project are typically hospital associations or state government agencies.

The type of data collected includes hospital discharge/visit records from inpatient, emergency department, or ambulatory surgery and services providers. Collected data elements maintained in the system include the date of service, type of medical service (procedure/surgery or diagnoses), length of hospital stay, costs, hospital size and location, patient date of birth, medical record numbers, and residential ZIP code. PII is used by data developers solely for the purpose of creating anonymized databases that can be released for research purposes. Direct contractors who act as developers and administrators are provided an AHRQ username and password for account access provisioning.

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

The HCUP Database System consists of multiple data storage and analytical servers connected on a secure internal network that house both the data and analytical programs. The servers are only accessible to authorized project staff. The HCUP databases stored in the system are based on the data collection efforts of data organizations in participating States that have partnered with AHRQ and maintain statewide data systems. The HCUP databases rely upon this data collection to 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. Direct contractors who act as developers and administrators are provided an AHRQ username and password for account access provisioning.

Does the system collect, maintain, use or share PII?

Yes

Indicate the type of PII that the system will collect or maintain.

Date of Birth

Medical Records Number

Note: Medical Record Numbers are encrypted.

Zip Code

User credentials

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

Employees

Patients

How many individuals' PII is in the system?

1,000,000 or more

For what primary purpose is the PII used?

The patient's date of birth is used to calculate age in years; a critical data element for research and aggregate statistical reporting. A zip code is used to identify the geographical location of patient care. Direct contractor PII is used to provision account access.

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.

Section 944(c) of the Public Health Service Act (42 U.S.C. 299c-3(c)) (“the AHRQ Confidentiality Statute”).

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

No

Identify the sources of PII in the system.

Email

Online

Government Sources

Within OpDiv

State/Local/Tribal

Identify the OMB information collection approval number and expiration date

OMB Control No. 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.

HCUP data received from partner organizations contain no directly identifying information and cannot be traced to a particular individual using the hospital records maintained within the HCUP system. Employees are notified when their IT 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.

HCUP data received from partner organizations is not collected for the purpose of identifying an individual, but rather to look at patient outcomes and treatments. PII collected is not attributed to a particular individual using the hospital records maintained within the HCUP system. If an individual made a request to opt out of collection or use of their PII, it would not be feasible to identify the records for removal. Direct contractors must provide their PII to provision account access within the system, and there is no ability to opt-out of the use of this information.

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

HCUP data received from partner organizations is not collected for the purpose of identifying an individual, but rather to look at patient outcomes and treatments. PII collected is not attributed to a particular individual using the hospital records maintained within the HCUP system, and this collection is secondary to the primary collection at partner organizations. Direct contractors that provide their information for system account provisioning are notified if their account access changes or is modified based upon their role.

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.

HCUP data contain no directly identifying information so it would not be possible to notify individuals whose PII is in the system and there is no process to resolve an individual's concerns. Direct contractors who believe that their information has been inappropriately obtained or used can contact the system owner to address and remediate their 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.

The database files are carefully documented, logged and reviewed annually with the system owner to ensure their integrity. In addition, when the medical record, date of birth, and zip code is processed to create work product (HCUP data products or analytical studies), extensive quality control and testing is conducted on the results to ensure accuracy and relevancy (particularly, no unauthorized disclosure of of this PII).

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

Administrators:

Direct contractor that supports maintenance of the system.

Developers:

Direct contractor that supports development and maintenance of HCUP databases.

Contractors:

Direct Contractors

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

Access to any data in HCUP is provided and approved by the system owner on an as-needed basis only, and only to those contractor employees that are specifically a part of the HCUP/AHRQ QI project, or agency employees who are part of the HCUP/AHRQ QI program, for the strict purposes of supporting HCUP activities.

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.

Access permission is restricted based on specific user roles and user groups as per HCUP/AHRQ QI project requirements. All user roles and user groups are managed and approved by the HCUP system owner.

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 Truven Health Analytics staff and contractors must take the AHRQ security and privacy awareness prior to being granted access to the system, and must then re-take the training on an annual basis. The training includes:

AHRQ Information Security & Privacy Awareness Training
HCUP Privacy Training
HCUP Data Confidentiality & Security Training
HHS Role-Based Training (Managers, IT Administrators, Executives).

Users must also sign data use agreements.

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

In addition to the training listed above, users must also complete the HCUP Data Use Agreement Training prior to accessing HCUP data.

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.

Data containing PII are reviewed annually and files older than two years are securely destroyed. 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 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 procedures, and least privilege principles.

Technical controls include windows security group policies (password, account management, system access, session timeout, etc.), two-factor authentication, detailed logging of user account activities, monthly vulnerability and configuration scans, anti-virus/malware protection, network monitoring, network segmentation / firewalls, and FIPS 140-2 encryption of data in transit.

Physical controls include restricted access to information system via electronic key cards, video camera surveillance, emergency power – uninterruptable power supply, interior location of information system (not situated near any external walls), inventory and tracking of information system components, and certified secure destruction of old storage media.