US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

04/18/2016

OPDIV:

AHRQ

Name:

Data Application Support System

PIA Unique Identifier:

P-1266702-532509

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 AHRQ Data Application Support System (ADASS) was developed to support web applications that provide data for several research centers within AHRQ. Specifically, the ADASS supports web applications that provide healthcare information from the Center for Financing, Access and Cost Trends (CFACT), Center for Delivery, Organization, and Markets (CDOM), and Center for Quality Improvement and Patient Safety (CQuiPS).

The ADASS hosts web applications for CFACT to provide health care leaders and policymakers with the information and tools they need to improve decisions on health care financing, access, coverage and cost. CDOM provides emerging research needs, manages a portfolio of research grants and contracts, conducts and publishes peer-reviewed research, and develops databases and software tools that can be used with those databases for researching acute and long-term treatment and the impact on treatment quality, outcomes, access, and cost.

CQuiPS conducts and supports user-driven research on patient safety and health care quality measurement, reporting, and improvement to develops and disseminate reports and information on health care quality measurement, reporting, and improvement.

The ADASS is hosted within the Social & Scientific Systems, Inc. (SSS) General Support System (GSS). Each of the hosted websites in ADASS are Minor Applications and part of the ADASS system operation.

Currently, six web applications are supported through ADASS; Medical Expenditure Panel Survey (MEPS); Healthcare Cost and Utilization Project (HCUPnet); National Healthcare Quality and Disparities Reports (NRQRDRnet); National Healthcare Internal Quality/Disparities Reports (IQDnet); State Snapshots(snaps10); and, Patient Safety Organization (PSO) Tracking System.

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

The ADASS collects information from numerous public federal sources. Once the collected data is manipulated in order to create aggregate and statistical data, analyses, reports, trends, and correlations on healthcare topics, it is maintained in ADASS and shared with the public via the six web applications described below.

MEPS hosts a survey that collects data from anonymous volunteers. MEPS surveys collect anonymous data about families and individuals, their medical providers, and employers across the United States.
HCUPnet collects aggregate statistics from hospital inpatient and emergency department source: number of discharges, length of stay, total charges, total costs, aggregate charges, percent died in the hospital, discharge status, percent admitted through the emergency department, percent admitted from another hospital, percent admitted from a long term care facility, etc.
NRQRDRnet collects data about age, sex, race, ethnicity, income, education, health insurance, activity limitations, and geographic location. IDQnet is an intranet version of the NQRDRnet. It collects the same type of information as QRDRnet internally. AHRQ researchers and analysts gain access to IDQnet by providing a first and last name and an AHRQ email; then they are assigned a username and password.

PSO is a national registry of patient safety organizations as part of a Federal requirement to implement the Patient Safety Act. PSO collects register information, such as component of parent organization, PSO street address, PSO phone, PSO fax, PSO website, PSO point of contact, PSO point of contact phone, and point of contact email. This information is directly entered into the system by the AHRQ's PSO team. This information is then provided through the web application for public consumption.

The State Snapshot web application is a data aggregation of publicly available information sourced from state level organizations. The type of information collected includes data about care affordability, care coordination, effective treatment, healthy living, person-centered care, diseases & conditions, cancer, cardiovascular disease, chronic kidney disease, diabetes, HIV and AIDS, mental health and substance abuse, and health insurance statistics. This data is then manipulated into state-by-state data profiles and provided through the web application for public consumption.

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

The ADASS collects information from numerous public federal sources. Once the collected data is manipulated in order to create aggregate and statistical data, analyses, reports, trends, and correlations on healthcare topics, it is maintained in ADASS and shared with the public via the six web applications described below. MEPS collects anonymous data about families and individuals, their medical providers, and employers across the United States that is used to provide the public data about types of healthcare, cost of services, quality of services, etc.

HCUPnet collects aggregate statistics from hospital inpatient and emergency department source. This information is then maintained and shared through HCUPnet to allow members of the public, researchers, and members of the academic community public to review health information collected by AHRQ. The shared data describes hospital and emergency care, disparities in care rendered to vulnerable subgroups of the population, data on the specific health services that anonymous Americans use, how frequently services are used, the cost of these services and how they are paid for, as well as data on the cost, scope, and breadth of health insurance.

NRQRDRnet collects data about age, sex, race, ethnicity, income, education, health insurance, activity limitations, and geographic location. This data is sourced from other AHRQ programs, the Centers for Disease Control and Prevention (CDC), the Health Resources and Services Administration (HRSA), the Indian Health Service (IHS), the National Institutes of Health (NIH), the Substance Abuse and Mental Health Services Administration (SAMHSA), the U.S. Census Bureau, and professional organizations such as the American Hospital Association (AHA), the National Hospice and the Palliative Care Organization (NHPCO) Family Evaluation of Hospice Care Survey (FEHCS). These anonymous data points are manipulated against trends in overall access to healthcare, the length of healthcare provision, and the disparities of current healthcare provision and then shared through NRQRDRnet for public consumption.
IDQnet is an intranet version of the NQRDRnet used by AHRQ researchers and analysts to perform research on healthcare provision and disparities therein. AHRQ researchers and analysts gain access to IDQnet by providing a first and last name and an AHRQ email; then they are assigned a username and password.
PSO collects PSO registration information for the purpose to registering these organizations to conduct business with AHRQ.

The State Snapshot web application is a data aggregation of publicly available information sourced from state level organizations. Once sourced, the data is manipulated into state by state profiles and maintained through the web application for public consumption.

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

Fax number

Usernames and passwords

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

Employees

Public Citizens

Vendor/Suppliers/Contractors

How many individuals' PII is in the system?

100-499

For what primary purpose is the PII used?

PSOs are public entities that register with AHRQ to become a certified reviewer of a variety of patient safety programs within the healthcare industry. PSOs only share a very limited amount of PII for registration. PSO collects registration information, such as PSO name, PSO parent organization details, PSO street address, PSO phone, PSO fax, PSO website, PSO point of contact name, PSO point of contact phone, point of contact fax and point of contact email. All information related to a PSO is directly entered into the system by the AHRQ. This information is available through the web application (https://pso.ahrq.gov/listed) for public reference.

IQDNet and PSO are the two applications used internally by AHRQ staff. These two applications require the logon to access the data. The administrator of these applications provide the login details to the authorized AHRQ staff. The UserIDs are created based on the user's email ID. ADASS maintains only userIDs and passwords of the users for IQDNet and PSO.

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

There are no secondary uses of the information.

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.

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

No

Not applicable.

Identify the sources of PII in the system.

Email

Online

Government Sources

Within OpDiv

Other Federal Entities

Non-Governmental Sources

Other

Identify the OMB information collection approval number and expiration date

OMB No. 0935-0143 (PSO only)

Is the PII shared with other organizations?

Yes

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

Within HHS

As part of the Patient Safety Act, AHRQ must provide the PSO name , PSO street address, PSO phone, PSO fax, PSO website, PSO point of contact, PSO point of contact phone, and point of contact email. This information is used to build a PSO profile that is shared for public consumption through the PSO web application.

Other Federal Agencies

AHRQ must provide the PSO name , PSO street address, PSO phone, PSO fax, PSO website, PSO point of contact, PSO point of contact phone, and point of contact email. This information is used to build a PSO profile that is shared for public consumption through the PSO web application.

State or Local Agencies

AHRQ must provide the PSO name , PSO street address, PSO phone, PSO fax, PSO website, PSO point of contact, PSO point of contact phone, and point of contact email. This information is used to build a PSO profile that is shared for public consumption through the PSO web application.

Private Sector

AHRQ must provide the PSO name , PSO street address, PSO phone, PSO fax, PSO website, PSO point of contact, PSO point of contact phone, and point of contact email. This information is used to build a PSO profile that is shared for public consumption through the PSO web application.

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

AHRQ is required to build, maintain, and share a list of patient safety organizations publicly, per requirements set forth in the Patient Safety Act.

Describe the procedures for accounting for disclosures.

Not applicable.

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 PSO Compliance Self-Assessment Guide states that "The Certification for Initial Listing form can be submitted at any time. The protections of the law are not in place until the entity is listed by AHRQ. The rule does not establish any deadlines for submission. There are no limits on the number of PSOs that can be listed." Any PSO who wishes to do business under the protection of the Patient Safety Act must register with AHRQ.

IQDnet users are notified by ADASS system administrators that only userIDs and passwords are collected to give access to the system.

PSO users are notified by ADASS system administrators that only userIDs and passwords arecollected to give access to 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.

Any PSO who wishes to do business under the protection of the Patient Safety Act must register with AHRQ. The information that is collected must be provided through the PSO web application as a matter of national public registry. The use of this information is mandatory if the PSO wishes to conduct business under the protection of the Patient Safety Act.

IQDnet users must provide limited personal information in order to access the system. Users that do not wish to provide their information will not have a username and password created to access the web application.

PSO users must provide limited personal information in order to access the system. Users that do not wish to provide their information will not have a username and password created to access the web application.

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

PSO points of contact are contacted directly and are notified of any changes within the system that affect their information. Additionally, PSO points of contact are notified when their PSO organization has been moved to a delisted status according to the PSO Compliance Self-Assessment Guide. PSOs may choose to withdraw their organization from the AHRQ PSO national registry.

IQDnet users are notified of any change in the system that will affect their ability to access the system by ADASS system administrators. Users may choose to discontinue access to the system as a result of the change.

PSO users are notified of any change in the system that will affect their ability to access the system by ADASS system administrators. Users may choose to discontinue access to the system as a result of the change.

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.

As a requirement of the Patient Safety Act, AHRQ is required to provide a national public registry of registered PSOs. The information is public. If any information becomes inaccurate, the PSO Compliance Self-Assessment Guide requires PSOs to notify AHRQ immediate upon the identification of an inaccuracy. AHRQ ADASS system administrators promptly review and resolve any inaccuracies with the information provided through the PSO web application.

IQDnet and PSO users notify ADASS system administrators if a username or password is inappropriately used or is inaccurate. ADASS system administrators will promptly address any inappropriate or inaccurate uses of information directly with the IQDnet and PSO users.

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

There are no periodic reviews of PII contained within the system. As a requirement of the Patient Safety Act, AHRQ is required to provide a national public registry of registered PSOs. The information is public. If any information becomes inaccurate, the PSO Compliance Self-Assessment Guide requires PSOs to notify AHRQ immediate upon the identification of an inaccuracy. AHRQ ADASS system administrators promptly review and resolve any inaccuracies with the information provided through the PSO web application. A change of the point of contact information for any PSO requires that the PSO alert AHRQ of the change.

IQDnet and PSO users notify ADASS system administrators if a username or password is inappropriately used or is inaccurate.

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

Users:

IQDnet users will access the web application to attain research data used to conduct AHRQ research activities.

Administrators:

SSS system administrators have access to the system to maintain all system and web application operations.

Developers:

SSS system developer have access to the system to develop and update web application code for the efficient use of the applications in the ADASS system.

Contractors:

Contractors, performing as administrators and developers, will access the system to perform those assigned duties.

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

SSS system administrators and administrators are contracted by AHRQ to conduct system administration and development support. As part of the contract individuals that support the ADASS contract must complete a Declaration for Federal Employment form (OMB 3206-0182) and a Request for Personnel Security and Badging Services form (HHS-828) prior to gaining any type of administrator or developer access to the system. The AHRQ Contract Officer Representative (COR) approves the SSS contract Program Manager who subsequently assigns access to the ADASS based upon minimum privileges that an individuals needs in order to complete a contracted function. Individuals on the contract are also approved by the AHRQ COR.

Two separate Active Directory (AD) forests manage all staff and user accounts. The credentials and rights by AD group have a one way AD trust established to allow accounts to log in as authorized. All hardware used by the system and supported applications is managed in accordance with federal government standards for configuration and common security policies established by the National Institute of Standards and Technology (NIST).

Some of the key physical controls in place for the system include 24 x 7 on-site professional security staff that will monitor access points and make regular rounds of physical security inspections; up to seven control points between building exterior and customer equipment; audits or biometric access-verification devices (hand-scanners or others); video monitoring of activity in protected areas; recordings are stored for 30-days; and, key management to ensure only authorized parties are allowed physical access.

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.

Any SSS contractors assigned as developers or administrators to support the ADASS are assigned roles and responsibilities that are approved by the SSS Program Manager and the AHRQ COR. Each role and responsibility is attributed to a level of system access, and this access is in turn limited to the level of PII access required to carry out the role. Once a role is completed, or is no longer needed, the level of access is removed based upon a need to know when the contractor is reassigned.

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 staff are required to take an annual HHS-approved security awareness course. Role-based training is supplied to pertinent personnel.

Required training are HHS Information Security and Privacy Awareness, HHS Role-Based training for Administrators, HHS Role-Based training for Managers, AHRQ Information Security and Privacy Awareness Training.

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

There are no additional training requirements.

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.

Process and guidelines are established at the department level and documented in HHS Information Security Program Policy, Section 4.4 ("Media Control"), August 2014. Specific to data collection, the PSO system follows NARA N1-510-09-001.

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

The technical controls used on the system include a protected network that only accessible for system administration and development by a trusted 3rd party contractor. Access to the ADASS is protected using two factor authentication, using a personal identity verification (PIV) card, to log in for system access.

Administrative, technical, and physical security controls required for the system are defined in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Rev 4, "Security and Privacy Controls for Federal Information Systems and Organizations." These controls strengthen the information systems and the environment in which it operates, and are reviewed on an annual basis.

For physical security, 24 x 7 on-site professional security staff monitor access points and make regular rounds of physical security inspections. Up to seven control points between building exterior and customer equipment, and audits or biometric access-verification devices (hand-scanners or others). Video monitoring of activity in protected areas; recordings are stored for 30-days. Key management to ensure only authorized parties are allowed physical access.

Identify the publicly-available URL:

HCUPnet: http://hcupnet.ahrq.gov
MEPS: http://meps.ahrq.gov
National Healthcare Quality and Disparities Integrated NRQRDR: http://nhqrnet.ahrq.gov
State Snapshots: http://nhqrnet.ahrq.gov/snaps11
PSO: https://psotracking.s-3.net
IQDNet: https://iqdnet.s-3.com

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 uner 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