

US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

06/14/2016

OPDIV:

OS

Name:

Health System Measurement Project

PIA Unique Identifier:

P-4566343-015364

The subject of this PIA is which of the following?

Minor Application (child)

Identify the Enterprise Performance Lifecycle Phase of the system.

Development

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.

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 Health System Measurement Project (HSMP) brings together trend data on a limited set of key health system measures from multiple data sources to provide a picture of the status of the U.S. health system.

The Project focuses on ten critical dimensions of our health care system covering the availability, quality, and cost of care, the overall health of Americans, and the dynamism of the system. The Project examines the evolution of these aspects of our system over time. It also assesses the status of these dimensions of the system with respect to subgroups of the population, with a particular emphasis on vulnerable populations.

Health & Human Services' Office of the Assistant Secretary for Planning and Evaluation has developed the Health System Measurement Project to ensure a robust monitoring system through which people inside and outside government can assess how the system is doing and identify areas that need improvement. One important purpose of the Project is to track the consequences of implementation of The Affordable Care Act across this broad set of dimensions of the health system.

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

The HSMP website is comprised of 250+ datasets. Each displays trend data over time related to specific health measures (e.g., Percentage of off-based physicians who have adopted electronic health records, or percentage of surgical patients receiving recommended care). All data is compiled from public sources and provided to HSMP twice annually from a core set of public health informaticians who work with HSMP. The datasets are provided to the HSMP system owner in an Microsoft Excel workbook format and contain no Personally Identifiable Information (PII) or Protected Health Information (PHI).

Socrata.com is the platform that currently hosts the datasets that are in an Excel workbook format as previously mentioned. Socrata supports the system owner in uploading the datasets so they can be made available to the visitors of the HSMP website. However, Socrata.com is a separate entity from HSMP and users do not sign up on Socrata.com for any access point to HSMP. When users view the data from the datasets in a graphical interface format, they do it within the HSMP website. Socrata delivers the data from its platform to HSMP through an application interface connection that happens in the background. No information on users is gathered during their visit to the HSMP website.

Only the System Owner and two contractors (Technical Lead and Drupal Developer) have access to HSMP as administrators. They are the only ones that use credentials (user names and passwords) to access the Administration area of the site. Session cookies are used to recognize the users' credentials when they are actively accessing the site. Persistent cookies are used to recognize the user when they return to the site and the identifier is the computer they are using and its IP address. Both cookies do not share, access or track to any PII.

For the System Owner the HHS email address is stored. For the two contractors their contractor email addresses are stored. The contractors are not direct contractors.

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

The Health System Measurement Project (HSMP) brings together trend data on a limited set of key health system measures from multiple data sources to provide a picture of the status of the U.S. health system.

The Project focuses on ten critical dimensions of our health care system covering the availability, quality, and cost of care, the overall health of Americans, and the dynamism of the system. The Project examines the evolution of these aspects of our system over time. It also assesses the status of these dimensions of the system with respect to subgroups of the population, with a particular emphasis on vulnerable populations.

On the HSMP site users can see year-over-year comparisons in graphs and charts for several health measures (e.g., Percentage of off-based physicians who have adopted electronic health records, or percentage of surgical patients receiving recommended care). Users can view the graphs and charts associated with the data presented. Session cookies are not being used and they (users of the system) are not being tracked.

Session cookies are only used for administrative access and are only used to recognize the administrators' credentials and to allow access to the administrative functions of the site. However, these cookies do not store or track any personal identifiable information.

For the System Owner the HHS email address is stored. For the two contractors their contractor email addresses are stored. The contractors are not 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

Username

Passwords

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

Vendor/Suppliers/Contractors

ASPE HSMP staff administrators

How many individuals' PII is in the system?

<100

For what primary purpose is the PII used?

Login into the system to administer the application.

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

N/A

N/A

N/A

Identify the sources of PII in the system.

Online

Government Sources

Within OpDiv

Non-Governmental Sources

Private Sector

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.

The system collects PII (user names and passwords) directly from the system owner and contractors that administer the HSMP website. Verbal notice is given by the HSMP system owner and contractor project manager that the PII is only gathered and stored for the purposes of accessing the HSMP site to perform administrative and maintenance functions. The collection is not governed by the Privacy Act.

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.

There is no opt-out feature since individuals have taken the affirmative action (opt-in) to allow the system to collect or use their PII (names, email addresses and passwords), they have granted permission for the use. It is required to access the system as an administrator.

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

The System Owner notifies system administrators of any material changes that will impact the existing access credentials or if additional credentials are needed that would require additional user names and passwords.

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.

In the event that PII has been inappropriately obtained, used, or disclosed, the affected person(s) would escalate this concern to the contractor project manager in writing. The contractor project manager would engage with the appropriate channels to investigate the root cause and work on a process to resolution.

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 integrity, availability, accuracy and relevancy of the data is ensured because the administrators (whose PII is contained in the system) are charged with reviewing, monitoring and ensuring that new accounts are setup and terminated as necessary. As a result ensuring outdated, unnecessary, irrelevant, incoherent, and inaccurate PII is removed from the system.

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

Administrators:

To log in as administrators.

Contractors:

to log in as administrators.

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

Designated System Administrator access is determined by the staffing of the project and is managed by the contractor project manager. The established administrative procedure is that System Administrators have access to each other's email addresses. However, they do not have access to each other's passwords.

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 level system controls are set to the least privilege for all administrators limited to the functions and information that is essential to administering or adding functionality to the HSMP site.

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.

There is no training and awareness provided since users know that the only purpose of the email address and name stored in the system is to allow administrative users to authenticate to access the system. All HHS employees and contractors are required to complete annual privacy and security training.

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

N/A

Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices?

No

Describe the process and guidelines in place with regard to the retention and destruction of PII.

The General Records Retention Schedule 4.3, Item 040 applies: Destroy immediately after copying to a record keeping system or otherwise preserving, but longer retention is authorized if required for business use.

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

The system is accessed over a Secure Socket Layer (SSL) authentication. The system only contains low level PII such as names and email addresses. This information is not publicly accessible. All PII is stored in the Relational Database Service (RDS) databases for the Health System Measurement Project /Strategic Planning System hosted Drupal instances. The only access to these databases is from the environment specific application servers. Those application servers additionally can only be logged in to through a Bastian Host that has an Internet Protocol (IP) address Whitelist. The connection to the Bastian Host and system is over Secure Shell (SSH). A person would also have to have an account and the appropriate permissions to access the PII.

Identify the publicly-available URL:

<https://healthmeasures.aspe.hhs.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?

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.

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?

No