Privacy Impact Assessment (PIA): OS - SHDR - QTR2 - 2020 - OS775329

Date: 7/1/2020

Acronyms

ATO - Authorization to Operate
CAC - Common Access Card
FISMA - Federal Information Security Management Act
ISA - Information Sharing Agreement
HHS - Department of Health and Human Services
MOU - Memorandum of Understanding
NARA - National Archives and Record Administration
OMB - Office of Management and Budget
PIA - Privacy Impact Assessment
PII - Personally Identifiable Information
POC - Point of Contact
PTA - Privacy Threshold Assessment
SORN - System of Records Notice
SSN - Social Security Number
URL - Uniform Resource Locator

General Information

PIA Name:	OS - SHDR - QTR2 - 2020 - OS775329	**PIA ID:**	1113367

Name of ATO Boundary:
OS - Synthetic Healthcare Database for Research -Cloud

PTA

PTA - 1A:	Identify the Enterprise Performance Lifecycle Phase of the system	Operations and Maintenance
PTA - 1B:	Is this a FISMA-Reportable system?	Yes
PTA - 2:	Does the system include a website or online application?	No
PTA - 2A:	Are any of the URLs listed accessible by the general public (to include publicly accessible log in and internet websites/online applications)?	
PTA - 3:	Is the system or electronic collection, agency or contractor operated?	Contractor
PTA - 3A:	Is the data contained in the system owned by the agency or contractor?	
PTA - 5:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	No
PTA - 5A:	If yes, Date of Authorization	
PTA - 5B:	If no, Planned Date of ATO	12/11/2020
PTA - 6:	Indicate the following reason(s) for this PTA. Choose from the following options.	New
PTA - 7:	Describe in further detail any changes to the system that have occurred since the last PIA	N/A

PTA - 8:	Please give a brief overview and purpose of the system by describing what the functions of the system are and how the system carries out those functions?	The system uses healthcare program data, employer-sponsored insurance data, and other health insurance information to the extent available for the purposes of conducting high-quality analyses, trend studies, predictive modeling, and promoting quality improvement efforts, among others, to improve healthcare quality and efficiency. The information is collected from governmental (e.g. HHS) and non-governmental sources (e.g. commercial data brokers). Administrators, developers, and contractors will be provided role-based access and permission of least privilege after completing various security and Personally Identifiable Information (PII) trainings. The data will be secured according to policies, procedures, and technologies consistent with Federal Information Processing Standards (FIPS) - 199 and National Institute of Standards and Technology (NIST) SP 800-53 Rev4 Moderate-rated systems. The category of individuals about whom information is being collected includes employees, public citizens, business partners/contacts (federal, state, and local agencies), vendors/suppliers/contractors, and patients.
PTA - 9:	List and/or describe all the types of information that are collected (into), maintained, and/or shared in the system regardless of whether that information is PII and how long that information is stored.	The collected information will include, but is not limited to military status, date of birth, medical records numbers, employment status, demographic variables, and variables relating to medical claims information (e.g. diagnosis codes, procedure codes, provider information, and other medical and payment information). Data destruction timelines and procedures will be implemented based on each individual Data Use Agreement's instructions. Typically these allow for the Data to keep for up to a year.
PTA -9A:	Are user credentials used to access the system?	Yes
PTA - 9B:	Please identify the type of user credentials used to access the system.	Non-HHS User Credentials Password Username
PTA - 10:	Describe why all types of information is collected (into), maintained, and/or shared with another system. This description should specify what information is collected about each category of individual	The Synthetic Healthcare Database for Research stores administrative health insurance data for the purposes of conducting analyses to improve healthcare quality and efficiency. The goal of the system is the production of high quality, timely accurate synthetic data files to Agency for Healthcare Research and Quality (AHRQ) and other stakeholders. The system collects user credentials from the registered system users, who are AHRQ and contractor staff in order to control access to healthcare administrative data. Information that is collected and maintained from the system users includes usernames, passwords, affiliated organization, phone number and e-mail addresses. This information is not shared beyond the system administrators.

PTA - 10A:	Are records in the system retrieved by one or more PII data elements?	Yes
PTA - 10B:	Please specify which PII data elements are used.	Date of Birth
PTA - 11:	Does the system collect, maintain, use or share PII?	Yes

PIA

PIA - 1:	Indicate the type of PII that the system will collect or maintain	E-Mail Address Phone numbers Military Status Date of Birth Medical Records Number Employment Status User Credentials Others - diagnosis codes, procedure codes, provider information, payment information, affiliated organization
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared	Business Partners/Contacts (Federal, state, local agencies) Employees/ HHS Direct Contractors Public Citizens Vendors/Suppliers/Third-Party Contractors (Contractors other than HHS Direct Contractors)
PIA - 3:	Indicate the approximate number of individuals whose PII is maintained in the system	Above 2000
PIA - 4:	For what primary purpose is the PII used?	The PII will be used for the purpose of creating analytically useful synthetic data files. The system also collects user credentials as part of it's multi-factor authentication in order to provide and control access to the system.
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research)	n/a
PIA - 7:	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.
PIA - 8:	Provide the number, title, and URL of the Privacy Act System of Records Notice (SORN) that is being used to cover the system or indicate whether a new or revised SORN is in development.	SORN is in development
PIA - 9:	Identify the sources of PII in the system	Government Sources Other Federal Entities Non-Government Sources Commercial Data Broker Private Sector
PIA - 9A:	Identify the OMB information collection approval number or explain why it is not applicable.	Not applicable because the system does not collect data directly from individuals. The data is

		provided by outside sources such as but not limited to, Healthcare Cost and Utilization Project (HCUP), Medical Expenditure Panel Survey (MEPS) and Network of Patient Safety Databases(NPSD)
PIA - 9B:	Identify the OMB information collection expiration date.	
PIA - 10:	Is the PII shared with other organizations outside the system's Operating Division?	No
PIA - 11:	Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason	There is no process in place to notify individuals that their personal information will be collected because the system does not directly collect PII from individuals. The PII obtained comes from data sources such as HCUP, MEPS, and NPSD.
PIA - 12:	Is the submission of PII by individuals voluntary or mandatory?	Voluntary
PIA - 13:	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 need for a method for individuals to opt-out because the system receives its information from sources other than individuals. Therefore it is the responsibility of HCUP, MEPS and NPSD to provide the methods for individuals to opt-out of the collection of their PII.
PIA - 14:	Describe the process to notify and obtain consent from the individuals whose PII is in the system when major changes occur to the system (e.g., disclosure and/or data uses have changed since the notice at the time of original collection). Alternatively, describe why they cannot be notified or have their consent obtained	If a major change occurs to how the system uses the data, an update would have to be made to the Data Use Agreements with the data sources.
PIA - 15:	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. If no process exists, explain why not	If an individual's PII was been inappropriately obtained, used, or disclosed the process is to report the details of the incident to the appropriate government personnel responsible for the system including HHS AHRQ Contracting Officer's Representative. The contractor will also report any data breaches to the data owners including Centers for Medicare and Medicaid Action Desk at 410.786.2580 or by email at cms_it_service_desk@cms.hhs.gov.
PIA - 16:	Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy. Please address each element in your response. If no processes are in place, explain why not	Any individual requesting access to the system is required to fill out an access request form identifying the role they will have on the system. User management activities are logged and user account login history is reviewed and inactive accounts are then disabled after 180 days of inactivity. All user accounts are reviewed and confirmed or updated on an annual basis.
PIA - 17:	Identify who will have access to the PII in the system and the reason why they require access	Users Administrators Contractors
PIA - 17A:	**Provide the reason of access for each of the groups identified in PIA -17**	

	Administrators -The system administrators, who are federal contractors, would have access to the names and contact information of users. This information would be used for system operations and maintenance. Contractors -The technical team users, who are federal contractors, would have access to the names and contact information of users. This information will be used to communicate information about the system to the users	
PIA - 17B:	Select the type of contractor	HHS/OpDiv Direct Contractor Third-Party Contractor (Contractors other than HHS Direct Contractors)
PIA - 18:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII	The system implements role based access. Any individual requesting access to the system is required to fill out an access request form identifying the role they will have on the system. The roles help enforce least privilege access. The Contracting Officer Representative (COR) has to approve the access and role.
PIA - 19:	Describe the technical methods in place to allow those with access to PII to only access the minimum amount of information necessary to perform their job	Roles are used to limit view and edit access through the system interface and back-end.
PIA - 20:	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 project team members take the HHS required security training and corporate security training to include training specific to handling and protecting PII.
PIA - 21:	Describe training system users receive (above and beyond general security and privacy awareness training).	Individuals that have security related positions or team members that have elevated privileges (e.g. network admins) are also required to take role based security training to inform them of their additional responsibility due to their specific roles which have additional risk.
PIA - 23:	Describe the process and guidelines in place with regard to the retention and destruction of PII. Cite specific NARA records retention schedule(s) and include the retention period(s)	The records will be retained in accordance with National Archive Records Administration (NARA) DAA-0510-2013-0003-0001.
PIA - 24:	Describe how the PII will be secured in the system using administrative, technical, and physical controls. Please address each element in your response	Administrative controls: Site administrators receive regular training in security rules and procedures for protecting PII. This training must be completed on an annual basis. Technical controls: Usernames and passwords utilizes hashing for encryption. User accounts are automatically locked after 60 days of inactivity. User accounts are logged off of the site after 15 minutes of inactivity. Physical controls: The facility is accessed controlled and has video surveillance
PIA - 25:	Describe the purpose of the web site, who has access to it, and how users access the web site (via public URL, log in, etc.). Please address each element in your response	N/A
PIA - 26:	Does the website have a posted privacy notice?	No
PIA - 27:	Does the website use web measurement and customization technology?	No
PIA - 27A:	Select the type of website measurement and customization technologies is in use and if it is used to collect PII	
PIA - 28:	Does the website have any information or pages directed at children under the age of thirteen?	No

PIA - 28B:	Is there a unique privacy policy for the website and does the unique privacy policy address the process for obtaining parental consent if any information is collected?	
PIA - 29:	Does the website contain links to non-federal government websites external to HHS?	No