Privacy Impact Assessment (PIA): OS - ARPMP - QTR2 - 2022 - OS1191852

Date Signed: 6/15/2022

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

Status:	Approved	**PIA ID:**	1453212
PIA Name:	OS - ARPMP - QTR2 - 2022 - OS1191852	**Title:**	OS - ASPR Recipient Performance Management Platform
OpDiv:	OS		

PTA

PTA - 1A:	Identify the Enterprise Performance Lifecycle Phase of the system	Initiation
PTA - 1B:	Is this a FISMA-Reportable system?	Yes
PTA - 2:	Does the system include a website or online application?	Yes

URL Details

Type of URL	List Of URL
Publicly accessible website with log in	https://uat-aspr.cs32.force.com/hhsaspr/s/

PTA - 3A:	Is the data contained in the system owned by the agency or contractor?	Agency
PTA - 5:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	No
PTA - 5B:	If no, Planned Date of ATO	11/1/2020
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	Original system - changes would not apply.

	that have occurred since the last PIA	
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 Assistant Secretary for Preparedness and Response (ASPR) Recipient Performance Management Platform is designed to support the management of one of the National Healthcare Preparedness Programs (NHPP) branch's Cooperative Agreements (CoAgs), which provides emergency supplemental funding to 53 hospital associations (recipients) to bolster their preparedness and response capacity and capabilities to COVID-19. The solution will be built upon Salesforce's Software-as-a-Service Community Cloud Plus platform and will serve various internal and external stakeholders involved with the CoAg. Key features of the ASPR Recipient Performance Management Platform include: • A home/landing page • Contact management to track and manage recipient and sub-recipient points of contact • Functionality for recipients to search for resources and guidance • Technical assistance (TA) capabilities that allow recipients to submit and track TA requests • Web-based forms that allow recipients to enter progress made against various performance measures • Ability for recipients to upload required documents
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.	Key data collected and maintained in system include: 1. Contact/user information 2. Performance management information and reporting (progress against measures) 3. Programmatic resources to support the recipient community including links to public facing

		websites such as ASPR TRACIE, phe.gov, templates to support the management of the cooperative agreement, etc. Technical assistance (TA) case requests and resolutions This information is collected and maintained to support ASPR NHPP's mission. None of the data collected or maintained are shared directly with any other government systems, etc. Data are used by ASPR NHPP for the purposes of programmatic decision making, aggregated and used to support required Congressional and Office of Management and Budget (OMB) reporting, etc.
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.	HHS User Credentials HHS/OpDiv PIV Card Non-HHS User Credentials Email address 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	Performance management data: System will collect information from recipients, including required performance measures that will help ASPR understand how each recipient is spending federal funding to support the ongoing COVID-19 response. Resources: System will house programmatic resources that support the hospital association recipients with the successful implementation of the cooperative agreement. Resources include links to public facing websites such as ASPR Technical Resources, Assistance Center, and Information Exchange (TRACIE), phe.gov, templates to support the management of the cooperative agreement, etc. Contact/user information: System will house information related to users including at organizational level (name of organization, Phone of organization, address of organization) and individual contact level (name, phone, email, title at organization)

PTA - 10A:	Are records in the system retrieved by one or more PII data elements?	No
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	Name E-Mail Address Phone numbers
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared	Employees/ HHS Direct Contractors Grantees
PIA - 3:	Indicate the approximate number of individuals whose PII is maintained in the system	51 - 200
PIA - 4:	For what primary purpose is the PII used?	The primary purpose of PII in the system is to manage cooperative agreement recipient and sub-recipient information and system user information
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research)	There are no secondary uses of this PII.
PIA - 7:	Identify legal authorities, governing information use and disclosure specific to the system and program	The Assistant Secretary for Preparedness and Response (ASPR) cooperative agreements are subject to HHS Administrative Requirements, which can be found in 45 CFR 75 and the Standard Terms and Conditions implemented through the HHS Grants Policy Statement located at https://www.hhs.gov/grants/grants/grants-policies-regulations/index.html. References in the HHS Grants Policy Statement to 45 CFR part 74 or 45 CFR part 92 have been superseded by 45 CFR 75
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.	Records/information are not retrieved by an individual's name or other unique identifier; therefore, this system is not subject to the Privacy Act and the Privacy Act System of Records Notice (SORN).
PIA - 9:	Identify the sources of PII in the system	Directly from an individual about whom the information pertains

		Email Government Sources Within the OPDIV
PIA - 9A:	Identify the OMB information collection approval number or explain why it is not applicable.	OMB #0990-0391
PIA - 9B:	Identify the OMB information collection expiration date.	11/30/2022
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	Prior to the launch of the system and in accordance with language provided in the funding opportunity announcement (FOA) and notice of funding opportunity (NOFO) each recipient was notified that recipient and sub recipient information was to be provided for purposes of cooperative agreement management. For internal federal users from ASPR and contractor users, the need to collect/obtain this information was communicated via ASPR National Healthcare Preparedness Program (NHPP) meetings and via emails from ASPR leadership.
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	If recipients have issue with the information being collected, they can notify their Field Project Officer.
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	The program will use existing communication mechanisms to communicate with individuals if major changes occur to the system. This includes direct contact with individual recipients via their Field Proje Officer, email communication, and via conference calls.
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	Initially, the individual recipient will have a conversation with their Field Project Officer and/or Assistant Secretary for Preparedness and Response (ASPR) program leadership to discuss concerns. Depending on the issue, ASPR may work with system support (e.g., contractors) to resolve. For example, if the data are inaccurate, contractor staff can correct this in the system. For matters dealing with suspected improper use, disclosure, etc., ASPR will work with the Information System Security Officer (ISSO) and other relevant parities as needed

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	**For data integrity and accuracy:** Salesforce has built in mechanisms to ensure that certain data entered into the system reflect expected information and to ensure consistency. Recipients and ASPR staff have the ability to request changes to their data if they see inaccuracies as well as make changes to their own PII directly. As a note, there are security and privacy mechanisms in place to ensure that recipients only see PII relevant to their organization and associated contacts (for example, a recipient from Montana can only see (and edit as needed) PII relevant to Montana organizations and associated contacts; they could not see information about California's or Florida's). **For data availability:** Data in the ASPR Salesforce platform will only be available to authorized and active users of the system based on the level of access granted to them by ASPR program leadership. Users of the system will always have access to their data as long as they are authorized to log into the system. **For data relevancy:** ASPR program leadership will perform a recurring assessment of data collected in the system to ensure that the minimum necessary data are collected in order to meet its mission.
PIA - 17:	Identify who will have access to the PII in the system and the reason why they require access	Users Administrators Developers Contractors
PIA - 17A:	Provide the reason of access for each of the groups identified in PIA-17	

		For recipient users of the system, ASPR leadership requested that each hospital associated recipient submit two (2) named users per hospital association. Following submission via email, each user was reviewed and approved by ASPR leadership. Each recipient user has the same basic role-based access to the platform, which includes access to PII that is restricted to information that is associated with their own organization, organizational contact information, and their own contact information. Internal users, including federal staff and contractors across multiple roles (administrators, developers, etc.) has also been approved to access the system by ASPR program leadership. Each individual's role determines their access to PII, per the response to PIA 17. For contractors, each individual signs a non-disclosure agreement and takes Confidential Information Management Plan (CIMP) training.
PIA - 17B:	Select the type of contractor	Grantees
PIA - 18:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII	For recipient users of the system, ASPR leadership requested that each hospital associated recipient submit two (2) named users per hospital association. Following submission via email, each user was reviewed and approved by ASPR leadership. Each recipient user has the same basic role-based access to the platform, which includes access to PII that is restricted to information that is associated with their own organization, organizational contact information, and their own contact information. Internal users, including federal staff and contractors across multiple roles (administrators, developers, etc.) has also been approved to access the system by ASPR program leadership. Each individual's role determines their access to PII, per the response to PIA 17. For contractors, each individual signs a non-disclosure agreement and takes Confidential Information Management Plan (CIMP) training.
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	As stated in PIA 16, Salesforce has role based security mechanisms. Based on one's role, this drives what PII a user can see and have access to in the system. For example, a recipient from Montana can only see (and edit as needed) PII relevant to Montana organizations and associated contacts; they could not see information about California's or Florida's.
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	Contractor staff (Deloitte) are required to take a variety of security and privacy training annually, including courses on maintaining federal information confidentiality and privacy, security, and on ethics and professional conduct. HHS employees take annual information security awareness training and (as needed) role based training

PIA - 21:	Describe training system users receive (above and beyond general security and privacy awareness training).	Users will receive basic training on the use of the system, which covers how to securely access the system (including use of multi-factor authentication) and role-based privacy and security mechanisms
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)	From a Salesforce technical perspective, active customer data stays on disk until it is deleted or changed. Deleted data is temporarily available (15 days) online from the recycle bin. Backups are rotated every 90 days (30 days for sandboxes); therefore, changed or deleted data older than 90 days (30 days for sandboxes) is unrecoverable. ASPR National Healthcare Preparedness Programs (NHPP) abides by the General Records Schedule 1.2: Grant and Cooperative Agreement Records. Please see https://www.archives.gov/files/records-mgmt/grs/grs01-2.pdf for more information. For the type of data stored in the system, the retention policy states data will be stored until three (3) years after the final action is taken on the file. ASPR NHPP will destroy PII immediately when it no longer necessary for the management of the cooperative agreement. For example, user data is deleted upon notification that the individual no longer requires access to the system. Organizational and individual contact data is deleted/destroyed when that organization is no longer is a recipient of ASPR funding.
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:** The Salesforce platform is only accessible to authorized and active users of the system based on the level of access granted to them by ASPR program leadership. Users of the system will always have access to their data as long as they are authorized to log into system. ASPR program leadership has established roles for each user of the system so that individuals only see PII relevant to their role. For example, recipients only see PII relevant to their own organization and associated contacts (e.g., a recipient from Montana can only

		see (and edit as needed) PII relevant to Montana organizations and associated contacts; they could not see information about California's or Florida's). System administrators, because their role is more expansive in the system, can see user and contact information across all organizations for the purposes of managing and maintaining the system. **Technical / Physical:** Salesforce has built in technical and physical controls to ensure data security and privacy. These include: 1) User profiles. We control the access to PII by customizing profiles. Within objects, organizations can then control the access users have to fields using field-level security. Sharing settings allow for further data access control at the record level. 2) Auditing and event monitoring. We track changes to fields and monitor user activity in Salesforce. 3) Multi-factor authentication. Users log in with a user name and password as well as enter in a one-time passcode. ASPR will be adopting the Okta platform in the coming weeks for secure identity management and access of the Salesforce platform. More information on Salesforce's inherent privacy and security controls are here: 1. Privacy Statement: https://www.salesforce.com/company/privacy/ For detail on privacy protection at Salesforce: http://content.trust.salesforce.com/trust/en/learn/protection/
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	The purpose of the system is to support the management of an ASPR cooperative agreement, including how recipients are tracking on major requirements of the cooperative agreement and how they are spending federal funding. Users that have access to this system are the 53 hospital association recipients (2 users for each hospital associations), approximately 25-30 ASPR staff users, and contractor staff users. Initially at go-live, each user (whether external or internal to ASPR) will log on to the system with a provisioned username and password as well as multi-factor authentication (using built-in Salesforce functionality). ASPR adopting Okta, a

		secure, identity management and authentication platform in the coming weeks; once in place, all users will authenticate into the system using Okta.
PIA - 26:	Does the website have a posted privacy notice?	Yes
PIA - 27:	Does the website use web measurement and customization technology?	No
PIA - 28:	Does the website have any information or pages directed at children under the age of thirteen?	No
PIA - 29:	Does the website contain links to non-federal government websites external to HHS?	No