US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

09/24/2013

OPDIV:

OS

Name:

Supply Chain Tracking Tool

PIA Unique Identifier:

P-9370759-260674

The subject of this PIA is which of the following?

Minor Application (stand-alone)

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?

No

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.

This is an initial PIA conducted pursuant to contract HHSO100201200036A awarded 9/29/2012.

Describe in further detail any changes to the system that have occurred since the last PIA.

This is the first PIA for the Supply Chain Tracking Tool. the contract is base plus 3 option years effective 9/29/2012.

Describe the purpose of the system.

The purpose of the system is to track vaccine production during its life cycle from manufacturing to distribution. The analysis of the data collected will improve the accuracy of vaccine production projections for decision makers in public health response scenarios.

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

The vast majority of the data elements in the system are technical and scientific data related to the manufacture of vaccines and drug products, phase 1 influenza, phase 2 other medical countermeasures drug products. The system also contains a small amount of PII in the form of contact information (name, phone numbers, and e-mail) of manufacturers and vendors of vaccines as well as government project officers. This PII would be necessary to conduct public health activities in the event of a pandemic.

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

SCTT is a Business Intelligence system for tracking vaccine production throughout its life cycle from manufacturing to distribution. The BI software tool uses S.A.P. Business Objects and Data Services to create reports and dashboards from vaccine product manufacturing data provided by pharmaceutical manufacturers. A business intelligence software tool helps analyze and visualize relevant data, so that timely decisions may be made.

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

Phone Numbers

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

Employees

Vendor/Suppliers/Contractors

Collection is limited to contact information.

How many individuals' PII is in the system?

<100

For what primary purpose is the PII used?

Business contact information is collected for use in the event that coordination among drug product manufacturers and government agencies would be necessary in a public health emergency, such as when responding to influenza pandemics. Drug product manufacturing is driven by the contractual relationship with the United States government, and so analyzing these issues may also involve coordinating with representatives from this industry.

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

None.

Identify legal authorities governing information use and disclosure specific to the system and program.

The "Pandemics and All-Hazards Preparedness Act" (PAPHA) was enacted in 2006 to improve the nation's ability to detect, prepare for, and respond to a variety of public health emergencies. PAPHA directs the Secretary of HHS to develop a National Health Security Strategy and update it every four years. The first NHSS was published in 2009. Page 23 of the NHSS is about capabilities for near real-time systems for capture and analysis of health security-related information, specifically to "Develop and use technologies and processes, including but not limited to automation, for the timely and efficient capture, transmission, processing, and analysis of information relevant to health security."

The President's Council of Advisors on Science and Technology (PCAST) released its "Report to the President on Re-engineering the Influenza Vaccine Production Enterprise to Meet the Challenges of Pandemic Influenza" on August 19, 2010. This guidance document also advised the Executive Branch to improve oversight of influenza vaccine production.

Also, the Public Health Emergency Medical Countermeasures Enterprise Review: Transforming the Enterprise to Meet Long-Range National Needs was released in August, 2010. The review includes a section on immediate needs related to pandemic influenza vaccines stating that "bulk vaccines need to be packaged and made ready for distribution." The SCTT tracking capability will facilitate decisions regarding the fill and finish of bulk vaccines in a pandemic."

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

No

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

Email

Government Sources

Within OpDiv

Non-Governmental Sources

Private Sector

Identify the OMB information collection approval number and expiration date

Not Applicable

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 business contact information will be collected and updated by the organizations' representatives in the normal course of business. Collection is limited to the minimum necessary to contact identify and contact the individual incident to public health response scenario. Notification is intrinsic to the nature of the businesses and the business relationships each organization has with the US government.

Is the submission of PII by individuals voluntary or mandatory?

Mandatory

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.

Business contact information is collected based on the business role the individual has with respect to medical countermeasures manufacturing contracts. For example, some contact information would be for government Project Officers or pharmaceutical manufacturers points of contact. Individuals in these roles share this contact information in order to execute their professional duties in coordinating public health responses.

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

No major changes to the system that would affect the rights or interests of the individuals are anticipated. In the event this were to occur, HHS could inform these individuals using the contact information we maintain. In general, for manufacturers, consent is implied in the nature of the contractual relationship with the pharmaceutical manufacturers in the course of normal business, and for government employees consent is implied in the nature of their roles as project officers, contracting officers, or Senior Executives that have duties related to public health emergency responses, and these activities are the core mission of ASPR, BARDA.

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.

The BARDA organization point of contact (Manufacturing, Facilities, & Engineering - MFE) division of BARDA will maintain and update the contact listing, and ensure that any inaccurate contact information is promptly corrected. The point of contact information is available through the Project Officer or Office of Acquisition Management, Contracts, and Grants Contract Officer. Any data subject that needs to have their information corrected or updated may do so by contacting any of these individuals.

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

Reviews will be performed ad hoc, e.g., when a significant change to the PII data occurs or if errors need to be corrected.

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

Users:

A limited number of key personnel int he program office will have access to the contact information, which will only be used to conduct public health responses

Administrators:

Ensure data integrity, conduct operations and maintenance

Developers:

Developers may have access to some PII incidental to developing the IT system.

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

The S.A.P. Business Intelligence system is limited to 25 users.
Access control will be role based, and limited to only those users who have a specific business need incident to developing or operating the system, or participating in a public health response scenario such as an influenza pandemic.

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.

Only the minimum amount of contact information is being collected, and access to that information is role-based. Access is limited by the implementation of information security controls in strict compliance with FISMA, such as requiring authentication of identify, and restricting access privileges.

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.

Annual privacy and information systems security awareness training is required to obtain and maintain system access.

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

User training materials are being developed by the contractor as part of the contractual deliverables.

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.

The records are unscheduled as of this date. Draft BARDA program record retention schedules have been submitted electronically to the National Archives by the OS Records Officer using the ERA system, and National Archives and Records Administration (NARA) appraisal/approval is pending. The system owner will retain a copy of the approved PIA in the Project Officer files, to be combined with the contract file per FAR upon contract closeout. NARA general record schedules (GRS) 3 - Routine Procurement Files applies to contractual procurement records.

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

The S.A.P. Business Objects business intelligence (BI) system is hosted at the tier one, military-grade Cyrus One Data Center in Houston, Texas. The SSAE 16 (formerly SAS 70) independent security controls auditors report is current. Defense in depth layers of security are provided, including digital closed circuit television, biometric authentication, and redundant systems for internet connections, power, cooling, and mechanical systems. The S.A.P. BI system has been installed, but there is no data in the system at this time as the system is in development. BARDA has hired an independent, third party team of Cybersecurity experts under an MOU effective 15 May 2013 to advise us on preparing the Security Certification & Accreditation package including advising on the appropriate admin, technical, and physical controls for full FISMA , NIST 800-53 compliance. The independent Cybersecurity team will also be conducting a third-party Security Test and Evaluation required for formal Authorization to Operate (ATO). The FIPS 199 risk categorization for this system is anticipated to be "moderate", selection of specific controls will depend on CIO approval of our Security C & A package. Specifics categories of security controls: Administrative - full Enterprise Performance Life Cycle (EPLC) compliance objectives were included in the Statement of Objectives (SOO), including administrative areas such as configuration management, change control, and preparation of security documentation. Technical - Authentication & Identity management, and access control, SQL database access and management controls are in place managed by the S.A.P. and Dyonyx sub-contractors. Physical - note the description above of the security controls in place at the Cyrus One Data Center re physical access to the hosting data center. Significantly, our Dyonyx L.P. partner has managed other major COTS (commercial-off-the-shelf) information systems for BARDA since Sept 2006, and was selected for their exceptional information security expertise, as they also consult on security for critical infrastructure for major energy companies. This Supply Chain Tracking Tool contract (for which Dyonyx and S.A.P. are subs, HealthCare Management Solutions is the prime) will benefit from the ATO renewal of 10 May 2013 for Barda Management Tools and MedicalCountermeasures.gov. The Security Test and Evaluation (ST&E) Reports for those systems were published 1 April 2013, and this contract will benefit from the information security lessons learned as they are directly applicable to this contract, because the hosting is in the same data center.