US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:
02/12/2014

OPDIV:
CDC

Name:
Countermeasure Response and Administration (CRA)

PIA Unique Identifier:
P-3656039-806029

The subject of this PIA is which of the following?
Minor Application (child)

Identify the Enterprise Performance Lifecycle Phase of the system.
Operations and Maintenance

Is this a FISMA-Reportable system?
No

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)?
Yes

Indicate the following reason(s) for updating this PIA.

Describe the purpose of the system.
CRA is a web-based application hosted by the CDC to manage specific actions taken to prepare for or respond to health events (e.g., pandemics, bioterrorism/radiation events) through the administration of various countermeasures to protect the health of potentially exposed people and provide for protected public health response teams. Countermeasures include vaccination and other types of drug prophylaxis, as well as non-drug actions such as patient follow up activities and isolation and quarantine monitoring. The recipients of the countermeasures may include potential responders from the public and private sector, identified exposed individuals, and the general public.

Describe the type of information the system will collect, maintain (store), or share.
CRA collects PII for the purpose of identifying individuals who have come into contact with infected persons. This enables Public Health Officials to coordinate dispensing vaccinations and medications by officials who have already had physical contact with infected person and to inform and contact public health officials in cases where they may have unknowingly come into contact with infected individuals.

CRA also collects PII for the purpose of following up and giving necessary vaccinations, medications, and potentially quarantine infected individuals and to monitor the progress of said individuals.

CRA collects grantee organization. PII patient vaccination records collected involuntarily, and vaccine data (batch and type). The data in the CDC/NIP Datamart is used to create various aggregate reports for the Grantees and for internal research at CDC.

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

The Countermeasure and Response Administration (CRA) system is a Web-based application that tracks patients and the countermeasures they receive during a public health event. CRA enables Global Administrators and Public Health Administrators to quickly set up the system, define parameters to tailor the system (including a field for the SSN), to input patient information and countermeasures, send/receive data, report aggregate counts, run reports, generate extracts, and view maps. When an event needs to be added to CRA, Global Administrators and Public Health Administrators are authorized to perform this task. A Global Administrator is a CDC representative responsible for supporting the system and providing assistance to jurisdictional users. He/she has full access rights to all CRA functionality and access rights to the data of all jurisdictions. A Public Health Administrator maintains administrative information for the top-level jurisdiction and may maintain jurisdiction, organization, staff, and user data for partner jurisdictions and subordinate jurisdictions. A CDC user is a CDC representative who is authorized to view and run reports at the partner jurisdiction level (these reports do not identify patients or organizations).

Does the system collect, maintain, use or share PII?
Yes

Indicate the type of PII that the system will collect or maintain.
Social Security Number
Date of Birth
Name
Driver's License Number
Mailing Address
Phone Numbers
Medical Records Number
Medical Notes
Foreign Activities
Passport Number
Ethnicity
Gender

Indicate the categories of individuals about whom PII is collected, maintained or shared.
Business Partner/Contacts (Federal/state/local agencies)
Patients

How many individuals' PII is in the system?
5,000-9,999

For what primary purpose is the PII used?
CRA collects public health official PII for the purpose of identifying individuals who have come in contact with infected persons; otherwise, CRA will not be able to meet its mission to coordinate dispensing vaccinations and medications in a crisis situation and public health emergency.

Collecting PII enables Public Health Officials to coordinate dispensing vaccinations and medications by officials who have already had physical contact with infected person and to inform and contact public health officials in cases where they may have unknowingly come into contact with infected individuals.

CRA collects patient PII for the purpose of following up and giving necessary vaccinations, medications, and potentially quarantine infected individuals and to monitor the progress of said individuals.

Describe the secondary uses for which the PII will be used.
CRA also allows Grantees to upload full sets of their data if they have a system that provides similar functionality to CRA. Non-identified data entered in the CRA application is combined with similar data that is uploaded and shared with the NIP datamart. The data in the datamart is used to create various aggregate reports for the Grantees and for internal research at CDC participating in the program.

Describe the function of the SSN.
To input patient information and countermeasures, send/receive data, report aggregate counts, run reports, generate extracts, and view maps.

Cite the legal authority to use the SSN.
The Public Health Service Act (PHSA), 42 U.S.C. §§ 201 et seq. (1994).

Identify legal authorities governing information use and disclosure specific to the system and program.
45 CFR 164.512(b) et seq.

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

Identify the number and title of the Privacy Act System of Records Notice (SORN) that is being use to cover the system or identify if a SORN is being developed.

SORN is In Progress

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains
In-Person

Government Sources
Within OpDiv
State/Local/Tribal

Non-Governmental Sources

Identify the OMB information collection approval number and expiration date
Not applicable

Is the PII shared with other organizations?
Yes

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

State or Local Agencies
Purpose State and local health departments for appropriate capability

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

Describe the procedures for accounting for disclosures.
N/A- CDC and CRA do not collect the data from individuals. They receive the data from state and local authorities (covered entities) who have collected it. Therefore, any disclosure accounting would be provided at that level.

Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason.
CRA does not notify nor obtain consent from any individuals whose PII is provided to the system from State Departments of Health and State Public Health Labs. CDC and CRA do not collect the data from individuals, but rather the data is received from state and local authorities (covered entities) who have collected it. Therefore, notices would be provided by the state entities.

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.
CDC and CRA do not collect the data from individuals. They receive the data from state and local authorities (covered entities) who have collected it. Therefore, any disclosure accounting would be provided at that level.

Process to notify and obtain consent from individuals whose PII is in the system when major changes occur to the system.
CDC and CRA do not collect the data from individuals. They receive the data from state and local authorities (covered entities) who have collected it. Therefore, any disclosure accounting would be provided at that level.

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.
CRA does not provide a complaint process for individuals who believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate. However, the patient may provide a complaint at the Physicians office, Health Dept, or other Point of Dispensing (POD). where their initial information was provided.

Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy.
A yearly review is performed on the PII elements in CRA in which the PIA is reviewed and submitted to the Chief Privacy Officer of the CDC. This also includes the SSN elimination/reduction worksheet. The PM also participates in regular briefings that include information on upcoming system changes.

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

Users:
Public Health officials – not those performing data entry – have access to IIF for those subjects within their geographical jurisdiction. This allows them to identify public health responders who are inoculated or otherwise protected from a current health threat. It also allows them to access reports on inoculation statistics for their jurisdiction.

Administrators:
This access is necessary to correct data integrity compromised by accident or malice. This access to view or change data is almost entirely incidental to the role.

Contractors:
The CRA administration staff are contract employees.

Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.
AC-6 Common Control Least Privilege

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.
CRA enforces least privilege through e-auth and within the application to ensure least privilege . Role-based ACLs and auditing as outlined in the system security plan. An individual user's access in terms of read/write/review within CRA is controlled by very strict role-based control. (Defined in CRA Security Approach which shows how CRA enforces the most restrictive set of permissions for authorized users at the application level based on job tasks..)

In terms of security audit logs, AHB maintains as a common control audit logs which are revealed only to authorized security personnel or administrators.

Documented in CRA Security Approach and CRA Requirements such as CRA Use Case/Wireframes (UCWFs) (listed and described in the Security Approach)_

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 users of the CDC systems receive annual Information Security and Privacy Awareness 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?
Yes

Describe the process and guidelines in place with regard to the retention and destruction of PII.
As stated in the CRA SSP, CRA has a policy and plan for retention and destruction of all CRA data, including PII, which is retained indefinitely in CRA.

Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.
This system is subject to CDC Certification and Accreditation process, and is accredited as a moderate system. It uses PKI to secure logins, complies with CDC policies and requirements for technical security. Technical controls are in place to minimize the possibility of unauthorized access, use, or dissemination of the data in the system: user identification, PIV including Smart Cards and CITGO keyfob remote access, strong frequently changed passwords, firewalls, SSN encryption, intrusion detection systems, and common access cards.

CRA is located in a physically secure area with guards, ID badges, and key cards.