US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

05/21/2020

OPDIV:

CDC

Name:

NCIRD Text Illness Monitoring (TIM)

PIA Unique Identifier:

P-7197654-293640

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?

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)?

No

Describe the purpose of the system.

NCIRD Text Illness Monitoring (TIM) is a secure mobile texting tool that facilitates symptom monitoring during an infectious disease outbreak. Monitoring conducted by public health officials has traditionally been conducted via telephone calls, which can be a time-consuming process requiring staff resources. CDC has developed TIM., an option utilizing two-way Short Message Service (SMS) /text messaging to aid in the process. Text messaging is an efficient method to identify, manage, and act on any infectious outbreak or pandemic-related activity (e.g., COVID-19, H1N1, etc.) among those who have been exposed or potentially exposed.

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

TIM will collect basic information (limited to name, phone number, zipcode and unique ID) of intended target audience to receive secure text messages. TIM will also hold information to responses to text messages (responses are in the yes or no form) if applicable.

In addition, TIM contains CDC Business Contact Information (BCI) and user credentials collected fromuser/system administrators in order to access the system.

Specifically, the information collected consists of userID and passphrase, as well as name and phone number.

Users/system administrators include CDC employees and direct contractors using HHS user credentials.

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

TIM is being used for the Coronavirus Disease 2019 (COVID-19) pandemic response. Use of TIM is voluntary for health departments. Consenting persons in participating jurisdictions will receive 2-5 text messages a day for up to 14 days asking if they have symptoms consistent with COVID-19. Health departments will immediately be alerted to any person in their jurisdiction that responds that they are experiencing symptoms and to any persons who fail to respond to two consecutive messages. Health departments would then follow up with individuals who are reporting symptoms or those that have been unresponsive.

TIM system includes a dashboard with summary information on number of persons being monitored, and information related to the alerts/notifications that public health needs to take action on (i.e., those that reply YES to a text indicating symptoms, those that have not responded to two consecutive texts). Jurisdictions can view the mobile phone number of participating individuals being monitored through the TIM system and the messages they send. There a two output reports in TIM. One report lists all the text responses received from the previous day, with each response tied to a phone number. The other report lists all the text responses received for the entire campaign, also tied to phone numbers.

TIM will collect basic information of intended target audience (limited to name, phone number, zipcode and unique ID) in order to receive secure text messages. TIM will also hold information to responses to text messages (responses are in the yes or no form) if applicable.

In addition, TIM contains CDC Business Contact Information (BCI) and user credentials collected from users/system administrators in order to access the system. Specifically, the information collected consists of userID and passphrase, name, and phone number.

Users/system administrators include CDC employees and direct contractors using HHS user credentials.

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

Yes

Indicate the type of PII that the system will collect or maintain.

Name

Phone Numbers

zipcode

Unique ID

User ID

Passphrase

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

Employees

Public Citizens

Business Partner/Contacts (Federal/state/local agencies)

How many individuals' PII is in the system?

10,000-49,999

For what primary purpose is the PII used?

The primary purpose of the PII collected is to facilitate public health outreach for those that meet public health follow-up criteria.

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

The secondary uses of the PII received are to analyze the responses and conduct contact tracing of the affected individuals.

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

Public Health Service Act, Section 301, "Research and Investigation," (42 U.S.C. 241); and Sections 304, 306 and 308(d) which discuss authority to maintain data and provide assurances of confidentiality for health research and related activities (42 U.S.C. 242 b, k, and m(d)).

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

In-Person

Email

Government Sources

State/Local/Tribal

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 state public health officials who originally collect the data from individuals are responsible for providing each individual with notice and choice.

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.

Access to the system requires the user credentials. If the user does not want the system to store their credentials, they can choose not to access the system.

The state public health officials who collect the data from individuals are responsible for providing each individual with notice and choice. If the individual does not want to provide his or her PII, it is not collected.

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

All persons using the system will receive text notification if any significant changes are made.

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 state public health officials who collects the data from individuals are responsible for providing each individual with notice and choice. Individuals are provided with a phone number of the health official to contact in case they have any questions or concerns regarding their PII. If the individual believes their PII information was inappropriately disclosed, obtained or misused, they can notify the health official who collected the information using text messages with their concerns.

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 PII data in the system (e.g., name, phone number, zip code and unique ID) are reviewed monthly for accuracy and availability. Regular data checks occur monthly to validate the integrity of the data. The data variables obtained by CDC ensures the information obtained is necessary for the stated analyses and project goals.

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

Administrators:

Administrators need access for data management.

Contractors:

Direct Contractors need access to the data for analysis and reports.

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

All users must be approved by the Business Steward based on their role, duties and responsibilities prior to gaining access to the data. Role Based Access Control (RBAC) is utilized. The roles are predefined and the users are assigned those roles as appropriate. Direct contractor roles are also defined.

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.

The data is accessible by the authorized personnel only. The Least privilege model is used. The Business Steward, or delegated system administrator review access reports on a monthly basis. They also review user credentials and audit access accounts annually.

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 CDC personnel are required to take CDC Privacy and Security Awareness Training at least annually.

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.

CDC Records Control Schedule CDC-02-2-41: federal record retention requirements, which specify that data files will be destroyed no sooner than 12 years after the completion of the Cooperative Agreement.

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

Administrative - Users will be granted access using a least privilege model by the Business Owner/Data Manager.

Technical - The back-end storage will be protected through the explicit access for those so authorized. Users who access the system on the CDC network shall be authenticated via PIV and username and passphrase.

Physical - The server is located in an access-controlled area with locked doors and security guards.