Privacy Impact Assessment (PIA): CDC - TMS - QTR2 - 2023 - CDC6736121

Created Date: 7/19/2023 11:55 AM Last Updated: 9/30/2024 8:01 PM

Copy PIA (Privacy Impact Assessment)

Do you want to copy this PIA ?

Please select the user, who would be submitting the copied PIA.

Instructions

Review the following steps to complete this questionnaire:

1) Answer questions. Select the appropriate answer to each question. Question specific help text may be available via the icon. If your answer dictates an explanation, a required text box will become available for you to add further information.

2) Add Comments. You may add question specific comments or attach supporting evidence for your answers by clicking on the icon next to each question. Once you have saved the comment, the icon will change to the icon to show that a comment has been added.

3) Change the Status. You may keep the questionnaire in the "In Process" status until you are ready to submit it for review. When you have completed the assessment, change the Submission Status to "Submitted". This will route the assessment to the proper reviewer. Please note that all values list questions must be answered before submitting the questionnaire.

4) Save/Exit the Questionnaire. You may use any of the four buttons at the top and bottom of the screen to save or exit the questionnaire. The button allows you to complete the questionnaire. The button allows you to save your work and close the questionnaire. The button allows you to save your work and remain in the questionnaire. The button closes the questionnaire without saving your work.

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:	CDC - TMS - QTR2 - 2023 - CDC6736121	**PIA ID:**	1679928
Name of Component:	CDC - Telework Management System	**Name of ATO Boundary:**	Telework Management System
Overall Status:		**PIA Queue:**	
Submitter:		**# Days Open:**	322
Submission Status:	Re-Submitted	**Submit Date:**	2/12/2024
Next Assessment Date:	N/A	**Expiration Date:**	1/1/2100
Office:		**OPDIV:**	CDC
Security Categorization:	Moderate	**OpDiv PIA ID:**	CDC6736121
Legacy PIA ID:		**Make PIA available to Public?:**	Yes

1:	Identify the Enterprise Performance Lifecycle Phase of the system.	Operations and Maintenance
2:	Is this a FISMA-Reportable system?	Yes
3:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	Yes
4:	ATO Date or Planned ATO Date.	3/5/2024
5:	Is the system or electronic information collection, agency or contractor operated?	Agency

PTA

PTA

PTA - 2:	Indicate the following reason(s) for this PTA. Choose from the following options.	PIA Validation (PIA Refresh)
PTA - 2A:	Describe in further detail any changes to the system that have occurred since the last PIA.	As part of an organization rebrand, the existing Telework Management System (TMS) was updated to rename the user interface to Workplace Flexibilities Management System (WFMS) however, the application url remained the same at telework.cdc.gov. There was no change to the system architecture, or the data collected for remote agreement and all references to the telework management system remains the same. Additionally, a new telework type "Remote Agreement" was added to the Request Type in TMS.
PTA - 3:	Is the data contained in the system owned by the agency or contractor?	Agency

PTA - 4:	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.	Telework Management system, also known as Workforce Flexibilities Management System, is an automated solution used for tracking and approval of telework requests by CDC employees. This allows the CDC to have the ability to satisfy annual calls by the Office of Personnel Management (OPM) and Health and Human Services (HHS) requesting data about telework participation at the CDC. In addition, TMS tracks employee location when teleworking. TMS is designed to allow users to manage and track requests for remote work from CDC employees, as well as provide responses to any data requests from organizations outside the CDC about remote work participation.
PTA - 5:	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.	Telework Management system, also known as Workforce Flexibilities Management System, contains CDC personnel names, date of birth, personal email, personal mailing address, personal phone number, medical notes, and medial numbers. The data is stored in the Management Information Systems Office (MISO) database and utilizes data from Data Management and Analytics Systems (DMAS). TMS accesses other application databases by using views from Administrative Codes, Learning Management System, Performance Management Appraisal System, and Time and Attendance. TMS uses Role Based Access Control (RBAC), so no username and passwords are required. This application does not collect PII however, TMS receives and maintains PII data from another CDC Internal system DMAS. The information that is collected in DMAS is mandatory and a condition of employment. DMAS is a separate system with its own PIA.
PTA - 5A:	Are user credentials used to access the system?	Yes, but the user credentials are maintained in a separate system (e.g., AD, AMS) and not collected or maintained by this system. The system providing credentials is
PTA - 5B:	Please identify the type of user credentials used to access the system.	

PTA - 6:	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.	Telework Management system (TMS), also known as Workforce Flexibilities Management System (WFMS), maintains employee information such as: name, email, mailing address, personal phone number, and medical information. This allows tracking of employee remote work requests and the associated remote location of the employee. Users: Employees have access to view their own remote agreement data for accuracy and submit documentation as an attachment if needed. Contractors: Contractors serving in the role of Telework Coordinator have access to view employee data for accuracy. Administrators: Users in the Telework Administrator role have access to PII data to ensure remote agreements and requests meet Telework requirements. Developers: Required for system development accuracy and validity.
PTA - 7:	Does the system collect, maintain, use or share PII?	Yes
PTA - 7A:	Does this include Sensitive PII as defined by HHS?	Yes
PTA - 8:	Does the system include a website or online application?	Yes
PTA - 8A:	Are any of the URLs listed accessible by the general public (to include publicly accessible log in and internet websites/online applications)?	No
PTA - 9:	Describe the purpose of the website, 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.	CDC employees access Telework Management system, also known as Workforce Flexibilities Management System via the url telework.cdc.gov Users: Employees have access to view their own remote agreement data for accuracy and submit documentation as an attachment if needed. Contractors: Contractors serving in the role of Telework Coordinator have access to view employee data for accuracy. Administrators: Users in the Telework Administrator role have access to PII data to ensure remote agreements and requests meet Telework requirements. Developers: Required for system development accuracy and validity. Users are restricted through Active Directory and the Role Based Access Control (RBAC) system. PII can only be accessed by authenticated users behind the firewall. Access is limited by user roles and access ranges.
PTA - 10:	Does the website have a posted privacy notice?	Yes
PTA - 11:	Does the website contain links to non-federal government websites external to HHS?	No

PTA - 11A:	Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?	
PTA - 12:	Does the website use web measurement and customization technology?	No
PTA - 12A:	Select the type(s) of website measurement and customization technologies in use and if it is used to collect PII.	
PTA - 13:	Does the website have any information or pages directed at children under the age of thirteen?	No
PTA - 13A:	Does the website collect PII from children under the age thirteen?	
PTA - 13B:	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?	
PTA - 14:	Does the system have a mobile application?	No
PTA - 14A:	Is the mobile application HHS developed and managed or a third-party application?	
PTA - 15:	Describe the purpose of the mobile application, who has access to it, and how users access it. Please address each element in your response.	
PTA - 16:	Does the mobile application/ have a privacy notice?	
PTA - 17:	Does the mobile application contain links to non-federal government websites external to HHS?	
PTA - 17A:	Is a disclaimer notice provided to users that follow external links to resources not owned or operated by HHS?	
PTA - 18:	Does the mobile application use measurement and customization technology?	
PTA - 18A:	Describe the type(s) of measurement and customization technologies or techniques in use and what information is collected.	
PTA - 19:	Does the mobile application have any information or pages directed at children under the age of thirteen?	
PTA - 19A:	Does the mobile application collect PII from children under the age thirteen?	
PTA - 19B:	Is there a unique privacy policy for the mobile application and does the unique privacy policy address the process for obtaining parental consent if any information is collected?	
PTA - 20:	Is there a third-party website or application (TPWA) associated with the system?	No
PTA - 21:	Does this system use artificial intelligence (AI) tools or technologies?	No

PIA

PIA

PIA - 1:	Indicate the type(s) of personally identifiable information (PII) that the system will collect, maintain, or share.	Name Email Address Phone numbers Date of Birth Mailing Address Medical Records Number Other - Free text Field - Medical Notes
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared.	Employees/ 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?	Telework Management System (TMS) maintains employee information such as: name, email, mailing address, personal phone number, and medical information. This allows tracking of employee telework requests and the associated telework location of the employee.
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research).	N/A
PIA - 6:	Describe the function of the SSN, Truncated SSN, and/or Taxpayer ID.	N/A . There are no SSNs collected or maintained in TMS.
PIA - 6A:	Cite the legal authority to use the SSN, Truncated SSN, and/or Taxpayer ID.	N/A. There are no SSNs collected or maintained in TMS.
PIA - 7:	Identify legal authorities governing information use and disclosure specific to the system and program.	Public Law 111-292, Telework Enhancement Act of 2010
PIA - 8:	Are records in the system retrieved by one or more PII data elements?	Yes
PIA - 8A:	Please specify which PII data elements are used to retrieve records.	Name Mailing Address Email Address Phone Number Date of Birth
PIA - 8B:	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.	OPM/GOVT-1, General Personnel Records
PIA - 9:	Identify the sources of PII in the system.	Government Sources Within the OPDIV
PIA - 10:	Is there an Office of Management and Budget (OMB) information collection approval number?	No
PIA - 10A:	Provide the information collection approval number.	
PIA - 10B:	Identify the OMB information collection approval number expiration date.	
PIA - 10C:	Explain why an OMB information collection approval number is not required.	OMB information collection approval number is required to avoid overburdening the public with data collection. No public information is collected in TMS.
PIA - 11:	Is the PII shared with other organizations outside the system's Operating Division?	No
PIA - 11A:	Identify with whom the PII is shared or disclosed.	
PIA - 11B:	Please provide the purpose(s) for the disclosures described in PIA - 11A.	

PIA - 11C:	List any agreements in place that authorizes the information sharing or disclosure (e.g., Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or Information Sharing Agreement (ISA)).	
PIA - 11D:	Describe process and procedures for logging/tracking/accounting for the sharing and/or disclosing of PII. If no process or procedures are in place, please explain why not.	
PIA - 12:	Is the submission of PII by individuals voluntary or mandatory?	Voluntary
PIA - 12A:	If PII submission is mandatory, provide the specific legal requirement that requires individuals to provide information or face potential civil or criminal penalties.	
PIA - 13:	Describe the method for notifying individuals that their information will be collected and how they can opt-out of the collection or use of their PII. If there is no option to object to the information collection, provide a reason.	The information is voluntary, however, as a condition of employment, employee information is mandatory. TMS pulls PII from other Application Services Branch (ASB) managed systems to pre-load employee data. Therefore, employee information is loaded and available whether an employee chooses to request a telework option or not.
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.	Users are notified by emails, announcements in the Consolidated Daily Announcements (CDA) emails, and/or notices posted to the CDC intra-net when significant changes to a system are made.
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.	User's may contact the TSB help desk or the CDC system that originated the data to submit a complaint. The helpdesk Technology Solutions Branch (TSB) will open a ticket and forward it to the appropriate entity to address the misuse or inappropriate collection of their PII.
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.	ASB managed applications are maintained within their respective databases. These feeds are updated every 24 hours in order to maintain the accuracy, relevance, timeliness and completeness of the PII.
PIA - 17:	Identify who will have access to the PII in the system.	Users Administrators Developers
PIA - 17A:	Select the type of contractor.	
PIA - 17B:	Do contracts include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices?	
PIA - 18:	Provide the reason why each of the groups identified in PIA - 17 needs access to PII.	**Users**: Employees have access to view their own data for accuracy and submit medical documentation as an attachment. As well as contractors serving in the role of Telework Coordinator. **Administrator**: User in the Telework Administrator role have access to PII data to ensure Telework agreements and requests meet Telework requirements **Developers**: Required for system development accuracy and validity.

PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Users are restricted through Active Directory and the Role Based Access Control (RBAC) system. PII can only be accessed by authenticated users behind the firewall. Access is limited by user roles and access ranges.
PIA - 20:	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.	Users are restricted through Active Directory and RBAC. PII can only be accessed by authenticated users behind the firewall. Access is limited by user roles and access ranges.
PIA - 21:	Identify the general security and privacy awareness training provided to system users (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.	Security Awareness Training (SAT) are required annually for all HHS employees and contractors as part of Security and Awareness Training.
PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	Telework Training for Users: all employees (including Commissioned Corps) utilizing TMS must complete Telework Training for Managers: managers with approval authority must complete this training in addition to the user training.
PIA - 23:	Describe the process and guidelines in place with regard to the retention and destruction of PII. Cite specific National Archives and Records Administration (NARA) records retention schedule(s) and include the retention period(s).	All official records are transferred or destroyed based on CDC record management policies and practices. The following records schedules apply to the system: GENERAL RECORDS SCHEDULE 5.2: Transitory and Intermediary Records Temporary. Destroy upon verification of successful creation of the final document or file, or when no longer needed for business use, whichever is later.
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: Records are maintained according with CDC's record control schedule and record control policy. This information is secured using the CDC/IS Active Directory authentication process and role-based application control. Technical: Monitored by the Network and IT security controls which are administered by TSB. The controls include user authentication/authorization via RBAC, firewalls and encryption. Data obfuscation is applied to user roles based on authorization. Unauthorized users do not have access to PII. Physical: Controls are managed by guards, ID badges, and key card restrictions.

Review & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	**Privacy Analyst Review Date:**	2/12/2024
Privacy Analyst Comments:	OpDiv Privacy Analyst: Joshua Mosios Status: Approved Date: February 12, 2024	**Privacy Analyst Days Open:**	

SOP Review

SOP Review Status:	Approved	**SOP Signature:**	
SOP Comments:	Approved on behalf of Beverly Walker	**SOP Review Date:**	2/22/2024
		SOP Days Open:	10

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	2/23/2024
Agency Privacy Analyst Review Comments:	Reviewer: Nestor Villafuerte This PIA is ready for SAOP review and approval.	**Agency Privacy Analyst Days Open:**	1

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	Archer Signature_Bridget Guenther.docx
SAOP Comments:		**SAOP Review Date:**	3/12/2024
		SAOP Days Open:	18

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
No Records Found				

Comments

Question Name	Submitter	Date	Comment	Attachment
PIA - 23	Data Feed Service, piafrmcdc	2/6/2024	This retention citation is no longer in use. Please provide an updated, accuate citation.	
PIA - 24	Data Feed Service, piafrmcdc	2/6/2024	The authentication process is a technical control. Please update.	
PIA - 1	Data Feed Service, piafrmcdc	9/30/2024	This System has been migrated within the OCIO ISB Infrastructure Services authorization boundary. All future updates should be made via the new Sub- Component application.	

Admin Section

Is OpDiv Privacy Analyst Approved ?:	1	**Is OpDiv Privacy Analyst Return ? :**	0
		Is SOP Return ?:	0
Is Agency Privacy Analyst Approve ?:	1	**Is Agency Privacy Analyst Return ?:**	0
Is SAOP Approved?:	1	**Is SAOP Return ?:**	0
Total Approved:	4	**Total Return:**	0
Total Approval Required:	4		

Miscellaneous Fields

Last Updated:	9/30/2024 8:01 PM	**History Log:**	View History Log