Save

Privacy Impact Assessment Form

v 1.47.4

Status: Draft | Form Number: F-11186 | Form Date: 2/8/2021 10:45:18 AM

	Question	Answer
1	OPDIV:	CDC
2	PIA Unique Identifier:	P-6144866-524316
2a	Name:	CDC Office 365 (CDC O365)
3	The subject of this PIA is which of the following?	○ General Support System (GSS) ◉ Major Application ○ Minor Application (stand-alone) ○ Minor Application (child) ○ Electronic Information Collection ○ Unknown
3a	Identify the Enterprise Performance Lifecycle Phase of the system.	Operations and Maintenance
3b	Is this a FISMA-Reportable system?	○ Yes ◉ No
4	Does the system include a Website or online application available to and for the use of the general public?	○ Yes ◉ No
5	Identify the operator.	◉ Agency ○ Contractor
6	Point of Contact (POC):	POC Title: Associate Director Shared Services Office POC Name: David Ausefski POC Organization: CSPO POC Email: add7@cdc.gov POC Phone: 412-386-6758
7	Is this a new or existing system?	◉ New ○ Existing
8	Does the system have Security Authorization (SA)?	○ Yes ◉ No
8b	Planned Date of Security Authorization	April 30, 2021 ☐ Not Applicable

Save

11	Describe the purpose of the system.	CDC has established this cloud computing Software as a Service (SaaS) for the purpose of providing the agency with
12	Describe the type of information the system will collect, maintain (store), or share. (Subsequent questions will identify if this information is PII and ask about the specific data elements.)	The CDC O356 system does not solicit, collect or request specific personally identifiable information (PII); however, it is expected that individuals or groups of individuals will include PII in the transmission of email messages. Likewise, users have
13	Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.	The CDC O365 is a Major Application (MA) supporting the transfer of messages among users of the system. Staff can send messages to other CDC staff members or externally to other
14	Does the system collect, maintain, use or share **PII**?	(•) Yes ( ) No
15	Indicate the type of PII that the system will collect or maintain.	☒ Social Security Number ☒ Date of Birth ☒ Name ☒ Photographic Identifiers ☒ Driver's License Number ☐ Biometric Identifiers ☒ Mother's Maiden Name ☒ Vehicle Identifiers ☒ E-Mail Address ☒ Mailing Address ☒ Phone Numbers ☒ Medical Records Number ☒ Medical Notes ☒ Financial Account Info ☒ Certificates ☒ Legal Documents ☒ Education Records ☒ Device Identifiers ☒ Military Status ☒ Employment Status ☒ Foreign Activities ☒ Passport Number ☒ Taxpayer ID EEO case related documents Other...(a) Active Directory credential information (UserID) and IP address to allow for mailbox synchronization and email delivery (b) Any information a user chooses to include in an email message such as unspecified PII

Save

16	Indicate the categories of individuals about whom PII is collected, maintained or shared.	☒ Employees ☒ Public Citizens ☒ Business Partners/Contacts (Federal, state, local agencies) ☐ Vendors/Suppliers/Contractors ☐ Patients Other	These categories only apply as a user may choose to include such information and unspecified PII in an email message, although it is not required by the information system. Within the Microsoft Teams component, external party information related to cases may be included in the documents. Most PII will consist of business contact information for professionals (such as attorneys, doctors, and representatives) and witnesses, who may be public citizens.
17	How many individuals' PII is in the system?	50,000-99,999	
18	For what primary purpose is the PII used?	The limited PII collected outside of transmitted message content is used primarily for authentication, inbox synchronization and message delivery. For example, Active Directory credential information is used by the system for authentication purposes only. The uses of PII transmitted in the context of messages is as varied as the functions and activities of CDC, from administrative to regulatory to educational and others. Within the Microsoft Teams component, EEO legal documents include complaints, settlements, alternative dispute resolution, and reasonable accommodations for CDC EEO cases. These documents contain PII, which may include names, mailing address, date of birth, medical records number, financial information related settlement agreements, and employment status. The primary purpose the PII is meet the standard information collected to adjudicate EEO matters and required for other documents in the EEO scope, such as reasonable accommodations and alternative dispute resolutions.	
19	Describe the secondary uses for which the PII will be used (e.g. testing, training or research)	None	
20	Describe the function of the SSN.	Not Applicable. SSN is not requested or required as part of the agency's or individuals' use of this system. SSNs may be transmitted in individual emails, but not according to any particular, defined use.	
20a	Cite the **legal authority** to use the SSN.	Not Applicable	

Save

21	Identify **legal authorities** governing information use and disclosure specific to the system and program.	5 U.S.C. Section 301 which provides authority for the agency to establish the organizations, procedures and tools necessary to perform its duties and pursue its mission. Information use and disclosure for this system is governed by the laws and regulations of the individual business practice that this system is used to conduct. Users work in various agency organizations that have different functions and are subject to different laws and regulations. Within the Microsoft Teams component, EEO legal documents include complaints, settlements, alternative dispute resolution, and reasonable accommodations for CDC EEO cases. Legal authorities include Executive Order 11478, 42 USC 2000e and 29 USC 633a.
22	Are records on the system retrieved by one or more PII data elements?	(•) Yes ( ) No
22a	Identify the number and title of the Privacy Act System of Records Notice (SORN) that is being used to cover the system or identify if a SORN is being developed.	Published: 09-90-0009, "Discrimination Complaints Records" Published: Published: ☐ In Progress
23	Identify the sources of PII in the system.	Directly from an individual about whom the information pertains ☒ In-Person ☐ Hard Copy: Mail/Fax ☒ Email ☒ Online ☒ Other Government Sources ☒ Within the OPDIV ☒ Other HHS OPDIV ☒ State/Local/Tribal ☐ Foreign ☒ Other Federal Entities ☐ Other Non-Government Sources ☒ Members of the Public ☐ Commercial Data Broker ☐ Public Media/Internet ☒ Private Sector ☐ Other
23a	Identify the OMB information collection approval number and expiration date.	Not Applicable

Save

24	Is the PII shared with other organizations?	(•) Yes ( ) No
24a	Identify with whom the PII is shared or disclosed and for what purpose.	☒ Within HHS Email address and content are shared as part of normal communication. Content of email varies with business function. EEO legal documents including complaints, settlements, alternative dispute resolution, and reasonable accommodations for CDC EEO cases may be shared with HHS EEO staff via the HHS iComplaints system, which is used to track EEO cases Department-wide. ☒ Other Federal Agency/Agencies Email address and content are shared as part of normal communication. Content of email varies with business function. ☒ State or Local Agency/Agencies Email address and content are shared as part of normal communication. Content of email varies with business function. ☒ Private Sector Email address and content are shared as part of normal communication. Content of email varies with business function. EEO and related case files may be shared or disclosed with professionals (attorneys, doctors, representatives) involved in a specific case, in order provide either legal representation or to provide expert analysis and opinions on the details of the case.
24b	Describe any agreements in place that authorizes the information sharing or disclosure (e.g. Computer Matching Agreement, Memorandum of Understanding (MOU), or Information Sharing Agreement (ISA)).	The agreements governing information exchange will vary with the business functions and purposes of exchanging email. Memorandum of Understanding and Information Sharing Agreements may be used as directed by policy with other HHS OpDivs with whom CDC interacts. For EEO and related cases, the CDC employee is required to complete a Designation of Representation Form in order to authorize information sharing and disclosure of case information to external professionals (attorneys, doctors, representatives).

Save

24c	Describe the procedures for accounting for disclosures	CDC O365 may be required to make such disclosures in the event that discovery is required pursuant to legal action; if needed to respond to public health or other national emergencies; or to investigate security or privacy incidents/ breaches. Such requests can be performed by an approved System Administrator; an accounting of responses for such disclosures will be managed through the existing management processes within CDC Information Technology Services Office (ITSO). For EEO and related cases, the Designation of Representation Forms are stored and accounted for outside of the CDC O365 system.
25	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 specific processes will vary along with the underlying business processes and practices that the use of email is supporting. CDC personnel are notified at the time of hire of the agency's use of their information in the context of their work for the agency. Personnel are also aware of the content of messages they send through the system. Upon logging on to the agency network prior to accessing the system, a warning banner advising personnel that they have no expectation of privacy when using government systems. External email transmitters may view CDC's web and privacy policies made available by the agency across all CDC.gov pages. For EEO and related cases, individuals and organizations which consulted an EEO counselor or filed a formal allegation of discrimination are aware of that fact. They may write the appropriate system manager indicated below or the general coordinator if the immediate system manager is unknown, regarding the existence of such records pertaining to them. The inquirers, as appropriate, should provide their name, date of birth, agency in which employed or agency in which the situation arose if different from employing agency, the approximate date, and the kind of action taken, when making inquiries about records. System Manager: Centers for Disease Control EEO Officer, Room 2405, Building 1, 1600 Clifton Road, NE., Atlanta, Georgia 30333
26	Is the submission of PII by individuals voluntary or mandatory?	(•) Voluntary ( ) Mandatory
27	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.	Voluntary: No PII data is specifically collected or used throughout the use of an email system; therefore, there are no notifications to users about PII data and no consent obtained from individuals. Obtaining consent and/or providing notification is part of the business processes underlying the use of an email service. Voluntary: For EEO and related cases, PII collection is required for case processing and adjudication. However, if the individual declines to share PII, he or she may not initiate an EEO complaint.

Save

28	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.	No major changes to CDC O365 are planned or anticipated. No PII data is specifically collected or used throughout the use of an email system; therefore, there are no CDC O365 specific notifications to users about PII data and no consent obtained from individuals. Obtaining consent and/or providing notification is part of the business processes underlying the use of an email service and is the responsibility of the organization administering the business process. For EEO and related cases, individuals and organizations which consulted an EEO counselor or filed a formal allegation of discrimination are aware of that fact. They may write the appropriate system manager indicated below or the general coordinator if the immediate system manager is unknown, regarding the existence of such records pertaining to them and if major changes have occurred to the system. System Manager: Centers for Disease Control EEO Officer, Room 2405, Building 1, 1600 Clifton Road, NE., Atlanta, Georgia 30333
29	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.	The process in place for resolving an individual's concerns is to: Contact the CDC Privacy Office at privacy@cdc.gov (or by phone at 770-488-8660) , reasonably identify the record and specify the information being contested, the corrective action sought, and the reasons for requesting the correction, along with supporting information to show how the record is inaccurate, incomplete, untimely, or irrelevant. For EEO and related cases, individuals may also write the appropriate system manager indicated below or the general coordinator if the immediate system manager is unknown: System Manager: Centers for Disease Control EEO Officer, Room 2405, Building 1, 1600 Clifton Road, NE., Atlanta, Georgia 30333

Save

30	Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy. If no processes are in place, explain why not.	Review of PII transmitted in the email system would not be efficient or appropriate. Data integrity is maintained at the level of the business process, or through maintenance of the applications that support business processes. The Active Directory information used by CDC O365 originates from a separate information system which has its own processes for maintaining integrity, availability, accuracy and relevancy. Agency-wide cybersecurity, physical security, continuing operations and other measures also support data integrity and availability and system functionality. Users are responsible for the accuracy and relevancy of PII they transmit over CDC O365. Within the Microsoft Teams component, EEO legal documents include complaints, settlements, alternative dispute resolution, and reasonable accommodations for CDC EEO cases. These documents contain PII, which may include names, mailing address, date of birth, medical records number, financial information related settlement agreements, and employment status. The EEO case managers periodically review the EEO legal documents (including PII) for assigned cases on an annual basis, to ensure that only those records that are relevant and necessary are maintained; that all records used to make a determination about an individual are sufficiently accurate, relevant, timely, and complete to make a fair decision; and that all records disclosed outside CDC are consistent with disclosure requirements of SORN 09-90-0009 "Discrimination Complaints Records, HHS/OS/ASPER"	
31	Identify who will have access to the PII in the system and the reason why they require access.	☒ Users	To send and receive email and perform duties. Within the Microsoft Teams
		☒ Administrators	CDC administrators provide Tier 4 Help Desk support which may require performing queries related to PII.
		☐ Developers	
		☒ Contractors	Offsite (indirect contractors) Microsoft Cloud Service provider support personnel (system administrators) have access to PII in order to provide
		☐ Others	
32	Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Users (i.e., those authorized to send and receive emails) and administrators that have completed CDC onboarding and personnel security processes, including security awareness and	

Save

33	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.	This is a standard email system, and emails are sent from user to specified recipients. Other parties (system administrators, contractors, users not party to a specific communication, etc.) will not have access to emails not specifically addressed to them, except as needed to perform support functions such as queries. Cloud providers in particular are not expected to have any access to the content of transmissions. CDC O365 system administrators with the appropriate permissions, who have signed Rules of Behavior and performed the required training, are able to access the contents of emails, for authorized purposes such as e-discovery or detection of breaches. Enforcement of this access is implemented by a Role Based Access Control methodology which uses a least privileges model to determine access ability based on job roles. Within the Microsoft Teams component, EEO legal documents include complaints, settlements, alternative dispute resolution, and reasonable accommodations for CDC EEO cases. Access to and use of these records are limited to those persons whose official duties require such access. The EEO Resource Manager determines which OEEO staff require access to specific Teams folders and documents and grants the minimum level of access accordingly.
34	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 are required to complete annual Information Security Training and Privacy Awareness Training.
35	Describe training system users receive (above and beyond general security and privacy awareness training).	Users are provided training regarding the basic concepts of accessing email and collaboration services offered by the CDC O365 cloud-based solution. CDC O365 Administrators are required to complete training in Security Incident Response, Contingency Planning and Operations, and Role-Based training.
36	Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices?	(●) Yes ( ) No

Save

37	Describe the process and guidelines in place with regard to the retention and destruction of PII. Cite specific records retention schedules.	Email messages and content that constitute a federal record which CDC is obligated to preserve will be subject to a variety of record retention schedules specific to each business use. Each agency user is responsible for adhering to the schedules that apply to the records under their control. Beyond PII maintained under an approved records schedule, users have the ability to archive messages containing PII on their workstation or in their mailbox indefinitely. Otherwise, the data retention policy on the CDC O365 storage arrays is 14 days. If a user deletes a message, at which time it is moved to the Deleted Items Recovery folder for 14 days. After this period, the deleted mail is stored in a purge folder for 14 days, during which time only authorized administrators can access it. The General Records Schedule (GSR) 5.5, item 10 (DAA-GRS-2016-0012-0001) and item 020 (DAA-GRS-2016-0012-0002) provide the specific retention schedules. GRS 5.5, item 10 Disposition Authority: DAA-GRS2016-00120001. Destroy when 3 years old, or 3 years after applicable agreement expires or is cancelled, as appropriate, but longer retention is authorized if required for business use. GRS 5.5, item 20 Disposition Authority: DDAA-GRS2016-00120002. Destroy when 1 year old or when superseded or obsolete, whichever is applicable, but longer retention is authorized if required for business use. Within the Microsoft Teams component: SORN 09-90-0009, "Discrimination Complaints Records, HHS/OS/ASPER", Retention and disposal: The records are retained for four years after final disposition, and are then destroyed. (See HHS Personnel Instruction 293-1, Exhibit X293-1-1, item 26a(1).)

Save

38	Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.	CDC O365 implements security controls to protect PII, as defined by OMB mandates, the Federal Information Security Management Act (FISMA), and NIST Special Publications (SP) 800-53, 800-37, 800-122, NIST Federal Information Processing Standards (FIPS) 200, 201, 199, 197, 140-2, and other associated documents as outlined by Federal Risk and Authorization Management Program (FedRAMP) (www.fedramp.gov). ADMINISTRATIVE CONTROLS: PII is secured within the system through the use of administrative controls in the form of mandatory security awareness and privacy training for all users; role-based training for privileged users; personnel screening as required by CDC; completion of contractual agreements and Rules of Behavior; and, users can encrypt email traffic, including those messages containing PII, in accordance with applicable CDC policies. TECHNICAL CONTROLS: Technical controls applied to CDC O365 include: continuous network/system monitoring; anti-malware; spam and email content filtering; FIPS 140-2 compliant encryption of data in transit; firewalls; Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Security Information and Event Management (SIEM), Data Loss Prevention (DLP); and multi-factor authentication. PHYSICAL CONTROLS: Physical controls include: Hosting within data centers which control and monitor physical access to the system components, including security guards, visitor control and auditing of access records; and, protection of power equipment and cabling, transmission medium, output devices and use of emergency power and shutoff systems as well as fire and water damage protection.
General Comments		Q10: The system will also include Equal Employment Opportunity (EEO) legal documents and other related documents.
OPDIV Senior Official for Privacy Signature	Jarell Oshodi -S	Digitally signed by Jarell Oshodi -S Date: 2021.02.18 14:21:43 -05'00'