Privacy Impact Assessment (PIA): CDC - ESSS - QTR2 - 2025 - CDC8723998

Created Date: 6/3/2025 8:01 PM Last Updated: 7/2/2025 4:00 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 - ESSS - QTR2 - 2025 - CDC8723998	**PIA ID:**	3264536
Name of Component:	CDC - Employee Support Services System	**Name of ATO Boundary:**	Employee Support Services System
Overall Status:		**PIA Queue:**	
Submitter:		**# Days Open:**	34
Submission Status:	Re-Submitted	**Submit Date:**	6/27/2025
Next Assessment Date:	N/A	**Expiration Date:**	7/1/2028
Office:		**OPDIV:**	CDC
Security Categorization:	Moderate	**OpDiv PIA ID:**	CDC8723998
Legacy PIA ID:		**Make PIA available to Public?:**	Yes

1:	Identify the Enterprise Performance Lifecycle Phase of the system.	Development
2:	Is this a FISMA-Reportable system?	Yes
3:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	No
4:	ATO Date or Planned ATO Date.	
5:	Is the system or electronic information collection, agency or contractor operated?	Contractor

PTA

PTA

PTA - 2:	Indicate the following reason(s) for this PTA. Choose from the following options.	New
PTA - 2A:	Describe in further detail any changes to the system that have occurred since the last PIA.	
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.	The purpose of the Employee Support Services System (ESSS) is to provide comprehensive Employee Assistance Program (EAP) Services to employees of the Centers for Disease Control and Prevention (CDC) which are workplace-based behavioral health services designed to help maintain and improve employee productivity and to help employees address the full range of personal problems. The Software as a Service (SaaS) platform is owned by Magellan Federal (a 3rd party vendor). The 3rd party vendor system is hosted and data is stored in the cloud (Salesforce Government Cloud Instances) as well as in 3rd party vendor facilities. Data is used for case management services requested by members (CDC employees, United States Public Health Service (USPHS), and family members) data & analytics used for contract specific reporting. No Protected Health Information (PHI) Personally Identifiable Information (PII) or Controlled Unclassified Information (CUI) is included in these reports.
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.	The types of information that is collected is as follows: Member demographic data points collected – All data is member provided and optional, caller does not need to share the demographic if they do not wish to. Name (Salutation, First, Middle, Last, Suffix) Mailing & Work Addresses Employer (self-reported) Phone & Mobile Number Email Division Contract Name Union Occupation Preferred method of contact Date of Birth Sex Member Type Salary Grade Primary Language if not English Consents – Permission to Leave voicemail, send email, and send text Case details of service request Call center intake details Risk Screening Provider notes Referrals Session details
PTA - 5A:	Are user credentials used to access the system?	
PTA - 5B:	Please identify the type of user credentials used to access the system.	Non-HHS User Credentials Username Password Email Address

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.	Data is collected when a member contacts the call center to request services. Data is collected from the member portal when a member self-registers for EAP services. Data is collected when a user creates an account on website. Data is collected when a user uses our website and their activity is sent to analytics to understand what pages were viewed and custom events to understand behaviors. Data is used for case management for services requested by members Data & Analytics for contract specific reporting (no PHI,PII or CUI) is included in these reports
PTA - 7:	Does the system collect, maintain, use or share PII?	Yes
PTA - 7A:	Does this include Sensitive PII as defined by HHS?	
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)?	
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.	The system is a cloud-based SaaS system hosted on the Salesforce Government Cloud Instances platform. The website is publicly available for members to find information, care and their benefits. Some benefits do require login in order to access eligibility and health plan activity information.
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?	Yes
PTA - 11A:	Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?	Yes
PTA - 12:	Does the website use web measurement and customization technology?	
PTA - 12A:	Select the type(s) of website measurement and customization technologies in use and if it is used to collect PII.	Session Cookies - Collect PII Other
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?	Yes
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 Medical records (PHI) Date of Birth Mailing Address Medical Records Number Employment Status User Credentials Other - Free text Field - Work Addresses; Employer (self-reported); Sex; Case details of service request; Call center intake details; Risk Screening; Provider notes; Referrals; Session details.
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared.	Employees/ HHS Direct Contractors Members of the public
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?	The primary purpose of the PII that will be collected is for user account creation via the EAP website; Member self-registration for EAP services; Member contacts the call center to request EAP services. Data is used for case management for services requested by members. The services offered to employees and their family members include counselling.
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research).	Data may be used for analytic metrics for contract specific reporting.

PIA - 6:	Describe the function of the SSN, Truncated SSN, and/or Taxpayer ID.	SSNs and/or Taxpayer ID are not used in this system.
PIA - 6A:	Cite the legal authority to use the SSN, Truncated SSN, and/or Taxpayer ID.	Not Applicable, SSNs and/or Taxpayer ID are not used in this system.
PIA - 7:	Identify legal authorities governing information use and disclosure specific to the system and program.	5 USC 301 Departmental regulations; 5 U.S.C. 7361, 7362, 7901 and 7904; and 44 U.S.C. 3101.
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.	The primary PII data element used to retrieve records is Name of individual. Secondary data elements potentially used to retrieve records are: User credentials (if the individual chose to establish an account); Phone & Mobile Number; Email Address.
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.	SORN 09-90-0010 Employee Assistance Program (EAP) Record
PIA - 9:	Identify the sources of PII in the system.	Directly from an individual about whom the information pertains Phone Email Online 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 not required because the full range of programmatic services is not offered to family (non-federal) members. The CDC employee will provide information, which would be an exemption from having an OMB information collection approval number.
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 vendor provides a Privacy Policy, Terms of Use; How to Opt-Out, and 'Your Ad Choices' as an automated tool for an individual to 'Opt-Out'. Your Ad Choices provides the option to select PII preferences for 'Opt-In' or 'Opt-Out'.
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.	The Privacy Policy requires that Privacy Notices are presented and acknowledged by the individual regarding the collection and use of PII data prior to the use of EAP services. If major changes occur in the system, individuals will be notified using the PII provided upon initial establishment of the account in order to obtain consent for continued use or to give them the option to opt out.
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.	Individuals who wish to file a complaint would be instructed to contact: eap@cdc.gov or call 770-488-7825.
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.	Periodic infrastructure and application vulnerability and data integrity scans are performed to verify data integrity of collected PII that resides in the system. Data quality checks are performed on a daily basis to verify the accuracy, relevance, timeliness, and completeness of PII by the vendor
PIA - 17:	Identify who will have access to the PII in the system.	Users Administrators Developers Contractors
PIA - 17A:	Select the type of contractor.	Third-Party Contractor (Contractors other than HHS Direct Contractors)
PIA - 17B:	Do contracts include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices?	Yes
PIA - 18:	Provide the reason why each of the groups identified in PIA - 17 needs access to PII.	Users only have access to their own personal data if an account has been established. Contractors may need access to PII to verify the members. Administrators may need access to verify the integrity of the data. Developers may need access to provide analytic metrics.
PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Access is driven by role-based permissions to limit access to PII. Permissions are assigned according to the principle of least privilege with the lowest level of permissions necessary to complete their job.

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.	The principle of 'Least Privilege' via 'Access Control' is employed, limiting the access to PII to only what is necessary to complete a task and/or perform job functions. Only authorized users have access to PII consistent with their job function and role. Access rights are provided via least privilege with appropriate segregation of duties.
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 and Privacy Awareness Training; Acceptable Use Policy; Information Technology Risk Management Policy; Vendor Risk Management Policy; Incident Response Policy; Data Protection Policy; Access Control Policy. All trainings occur annually.
PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	Users receive role-based job function training annually.
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).	General Records Schedule 2.7; Item 090 ; (Disposition Authority) DAA-GRS-2017-0010-0014 (Record Description) Employee Assistance Program (EAP) counseling records. Records of individuals who have sought or been referred to counseling services provided through the Employee Assistance Program (EAP). May include records of family members and dependents. (Disposition Instruction) Temporary: Destroy once employee has met condition(s) specified by agreement or adverse action or performance-based action case file has been initiated.
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: Cybersecurity Policy and annual privacy training that addresses proper data handling aspects of PII data within the system. Technical: The PII is secured in the system using implemented configuration of encryption technology, user authentication/authorization, cryptographic keys, network and boundary protections, automatic time-outs and logoffs. Additionally, Role Based Access Control is used to ensure that only those with a need to know for their job duties and are providing services to an individual have access to the data. Physical: Physical controls are administered by the use of facility access controls, which are used to prevent unauthorized intrusions and environmental/natural hazards, including locked doors and security guards.

Review & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	**Privacy Analyst Review Date:**	6/27/2025
Privacy Analyst Comments:		**Privacy Analyst Days Open:**	

SOP Review

SOP Review Status:	Approved	**SOP Signature:**	
SOP Comments:	Approved by Beverly E Walker, SOP	**SOP Review Date:**	6/27/2025
		SOP Days Open:	0

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	7/2/2025
Agency Privacy Analyst Review Comments:	7/2/2025 This PIA is read for SAOP review and approval. CDC confirmed the following responses for the following PTA question that didn't sync: PTA-7A: Does this include Sensitive PII as defined by HHS? 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)? Yes PTA-12: Does the website use web measurement and customization technology? Yes PTA-12A: Select the type(s) of website measurement and customization technologies in use and if it is used to collect PII. Other technology – local session storage for user's email once logged in Session Cookies- Do Not Collect PII	**Agency Privacy Analyst Days Open:**	5

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	Archer Signature Page.docx
SAOP Comments:	Approved on behalf of the SAOP	**SAOP Review Date:**	7/2/2025
		SAOP Days Open:	0

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
7-2-2025 EMAIL_RE_ CDC - ESSS - QTR2 - 2025 - CDC8723998 Return Questions.pdf	243850	.pdf	7/2/2025 1:20 PM	0

Comments

Question Name	Submitter	Date	Comment	Attachment
PIA - 1	Data Feed Service, piafrmcdc	5/30/2025	Please include all PII noted in PTA 5 e.g. Mailing & Work Addresses, Employer (self-reported), and Sex.	
PIA - 2	Data Feed Service, piafrmcdc	5/30/2025	Who are the patients? if they are not CDC patients and just employees then please remove patients. If information about family members of employees is included within this system, please include members of the public.	
PIA - 4	Data Feed Service, piafrmcdc	5/30/2025	Please check for grammar, also include the services that ESSS offers to employees and their family members, etc. counselling and other services that make medical notes and records essential to be kept within this system	
PIA - 5	Data Feed Service, piafrmcdc	5/30/2025	Please assume the reader has no previous knowledge of privacy and cybersecurity. For these reasons, always do the following: o Write in complete sentences. o Never include sensitive information (e.g., server locations and encryption software). o Avoid the use of technical jargon.	
PIA - 8A	Data Feed Service, piafrmcdc	5/30/2025	Please remove date of birth	
PIA - 8B	Data Feed Service, piafrmcdc	5/30/2025	Since records are retrieved by a Personal identifier as identified in PIA 8A, a SORN is applicable. Please check with the program to determine if an existing SORN can be applied based on the information collected by this system.	
PIA - 10	Data Feed Service, piafrmcdc	5/30/2025	Since earlier discussions determined that information about family members of employees is retained in this system, an OMB number is applicable, please check with the program to determine if an existing OMB can be applied to this system.	
PIA - 10C	Data Feed Service, piafrmcdc	5/30/2025	OMB is not required when the information is only about Federal	

			employees, please update response based on review of PIA 10.
PIA - 13	Data Feed Service, piafrmcdc	5/30/2025	Please explain in detail the process of opt-out in a way that the general public will understand.
PIA - 14	Data Feed Service, piafrmcdc	5/30/2025	Please review the question and provide a clear explanation of how notice is provided when major changes occur in the system.
PIA - 15	Data Feed Service, piafrmcdc	5/30/2025	Please review the question and provide a clear explanation of how an individual's concern is addressed.
PIA - 16	Data Feed Service, piafrmcdc	5/30/2025	Please provide an explanation of the administrative process not just the technical processes that are in place to ensure that the PII within the system is accurate. Examples are periodic reviews by a data steward etc. Please explain in words that will be clear to the general public.
PIA - 17	Data Feed Service, piafrmcdc	5/30/2025	Since vendors are mentioned in PIA 13, include contractors if applicable. Review to ensure that Developers and Administrators do not also have access to this system.
PIA - 18	Data Feed Service, piafrmcdc	5/30/2025	Please update if PIA 17 is updated.
PIA - 19	Data Feed Service, piafrmcdc	5/30/2025	Please add more details, what are these administrator controls? e.g. add in role based and least privileged as applicable.
PIA - 21	Data Feed Service, piafrmcdc	5/30/2025	Please include frequency of trainings for each training listed e.g. annually. Please remove all trainings already identified in PIA 22 so there is no repetition.
PIA - 22	Data Feed Service, piafrmcdc	5/30/2025	Please include frequency of trainings.
PIA - 23	Data Feed Service, piafrmcdc	5/30/2025	Please contact your program and identify the right NARA schedule control number for this system and include the retention period details within that schedule.
PIA - 24	Data Feed Service, piafrmcdc	5/30/2025	Please include a sentence each for Administrative, Physical and Technical controls. Please remove the reference to FIPS 140-2, this is too detailed.

PIA - 1	Data Feed Service, piafrmcdc	6/25/2025	Please also include the following in the free text since depending on the context, they could include PII and PHI that can potentially cause harm or embarrassment. Case details of service request Call center intake details Risk Screening Provider notes Referrals Session details
PIA - 2	Data Feed Service, piafrmcdc	6/25/2025	Are the individuals listed as patients, identified as patients within CDC clinics or partner clinics? if they are just employees and are not using CDC clinic facilities, then they should not be called patients. Please explain the context of the use of patients here within the notes section.
PIA - 7	Data Feed Service, piafrmcdc	6/25/2025	The HHS SORN 09-90-0010 lists the following authorities below, please add them to the list. 5 U.S.C. 7361, 7362, 7901, 7904; 44 U.S.C. 3101.
PIA - 8B	Data Feed Service, piafrmcdc	6/25/2025	Please explain the relevance of this SORN 09-40-0002 Public Health Service (PHS) Commissioned Corps Medical Records and its applicability to this system. The SORN for EAP listed by HHS can be found here, please review the SORN and update as applicable.
PIA - 13	Data Feed Service, piafrmcdc	6/25/2025	Can you please provide a brief description of the how to opt-out choices available through the vendor.
PIA - 14	Data Feed Service, piafrmcdc	6/25/2025	Please provide a brief summary of the choices available via the security and privacy policy for opt-in/opt-out.
PIA - 15	Data Feed Service, piafrmcdc	6/25/2025	Please review the question and provide a summary of the processes available for an individual to resolve issues identified with their PII.
PIA - 16	Data Feed Service, piafrmcdc	6/25/2025	Please also list any administrative reviews in place that address the validity of the PII in the system e.g. periodic reviews by a data steward to ensure removal of employees that are no longer with CDC etc.
PIA - 19	Data Feed Service, piafrmcdc	6/25/2025	I made some grammatical updates to the sentence provided.

PIA - 24	Data Feed Service, piafrmcdc 6/25/2025	Added this sentence to the administrative control: "The principle of least privilege is employed and all access to PII is role- based. Added this sentence to physical controls "which include locked doors and security guards."
PIA - 9	Data Feed Service, piafrmcdc 6/25/2025	I believe online should also be applicable here since PIA 4 says "The primary purpose of the PII that will be collected is for user account creation via the EAP website; Member self-registration for EAP services"
PIA - 8A	Data Feed Service, piafrmcdc 6/26/2025	Please identify which of these is the primary retrieval identifier (only one) and list it as such? Then list the others as Secondary.
PIA - 14	Data Feed Service, piafrmcdc 6/26/2025	This statement, "The SORN will also be updated if major changes occur" is not responsive since the cited SORN is not CDC's but an HHS SORN. Keep in mind that your response should describe actions that you can and should take that are within your purview. In your response @Q13, you reference Privacy Policy, Terms of Use, Opt-In/Out methods... all of which are in your purview. Think about how significant changes might impact an individual or their decision to surrender their info and how you can/should use any of those areas to convey any significant changes.
PIA - 18	Data Feed Service, piafrmcdc 6/26/2025	You state: "User may need access to PII to amend as necessary." This part of your response seems incomplete... what is it that is to be amended?
PIA - 24	Data Feed Service, piafrmcdc 6/26/2025	You wrote: Administrative: Records are maintained in accordance with CDC’s record control schedule and record control policy. The principle of least privilege is employed and all access to PII is role- based. Reviewer Comment: These controls include administrative policies, actions and procedures that are designed to manage the selection, development, implementation and maintenance of the security measures designed to protect the PII. Examples: Training requirements, any policies specific to the system use; risk analysis and log-in monitoring. This part, " The principle of least privilege is

			employed and all access to PII is role-based." is more akin to a technical control. Technical: You wrote- Monitored by Magellan's IT security controls. The controls include user authentication/authorization encryption. Reviewer Comment: "Magellan's IT security controls" is a specific branding and should not be stated as such. Talk about the technology, policies and procedures that is used to protect the PII and control access to it with no reference to a specific branding; doing so may enable a roadmap to bypass the controls. Instead, present your response in generic terms like encryption, automatic logoff, 2-factor authentication, etc. Physical: You wrote: This is a cloud-based system, physical controls are administered by the infrastructure vendor which include locked doors and security guards. Reviewer Comment: That this is a cloud-based system and specifying by whom/how the infrastructure is administered is irrelevant. You should simply state that the there are facility access controls used to prevent unauthorized intrusions and environmental/natural hazards, including locked doors and security guards.
PIA - 1	BLAND, CRYSTAL	7/2/2025	CDC confirmed the following responses for the following PTA question that didn't sync: PTA-7A: Does this include Sensitive PII as defined by HHS? 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)? Yes PTA-12: Does the website use web measurement and customization technology? Yes PTA-12A: Select the type(s) of website measurement and customization technologies in use and if it is used to collect PII. Other technology – local session storage for user's email once logged

	in Session Cookies- Do Not Collect PII

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:	7/2/2025 4:00 PM	**History Log:**	View History Log