




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:	OS - ADTP - QTR1 - 2025 - OS2340667	PIA ID:	3233170
Name of Component:	OS - ASPR Disaster Telemedicine Platform	Name of ATO Boundary:	ASPR Disaster Telemedicine Platform
Overall Status:		PIA Queue:	
Submitter:		# Days Open:	108
Submission Status:	Submitted	Submit Date:	5/29/2025
Next Assessment Date:	N/A	Expiration Date:	6/8/2028
Office:		OPDIV:	OS
Security Categorization:	Not Rated	OpDiv PIA ID:	OS2340667
Legacy PIA ID:		Make PIA available to Public?:	No
1:	Identify the Enterprise Performance Lifecycle Phase of the system.		Initiation
2:	Is this a FISMA-Reportable system?		No
3:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?		No
4:	ATO Date or Planned ATO Date.		6/30/2025
5:	Is the system or electronic information collection, agency or contractor operated?		

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.	<p>This is a Disaster Telemedicine platform designed to provide comprehensive support for healthcare delivery during disaster scenarios. Key functions of the system include:</p> <ol style="list-style-type: none"> 1. Telemedicine services. 2. Patient record management also known as Emergency Medical Records (EMR). <p>Medical information, including demographic details, medical history, treatment plans, and prescriptions, is collected about patients. This information is medically necessary to provide appropriate care and treatment of patients.</p>

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.	<p>1. User information such as email address, username and passwords for credentialing and permission.</p> <p>2. Medical information, including demographic details, medical history, treatment plans, and prescriptions, is collected about patients.</p> <p>All information collected on the platform will be securely stored in encrypted access controlled gov cloud. The information will be stored for the duration per HHS ASPR GUIDELINES (as long as the personnel has authorized access to the system) or until the United States Government (USG) ASPR directs otherwise and the personnel is terminated or no longer has authorized access to the system. This information is not shared with another system.</p>
PTA - 5A:	Are user credentials used to access the system?	Yes
PTA - 5B:	Please identify the type of user credentials used to access the system.	<p>HHS User Credentials</p> <p>HHS Email Address</p> <p>HHS Username</p> <p>Password</p> <p>Non-HHS User Credentials</p> <p>Username</p> <p>Password</p> <p>Email Address</p>
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.	<p>Information is collected for the purpose of:</p> <p>1. Credentialing and permission: Information such as username, passwords, roles and access are collected to ensure only authorized users can access the system.</p> <p>2. Patient care: medical information, including demographic details, medical history, treatment plans, and prescriptions, is collected about patients. This information is medically necessary to provide appropriate care and treatment of patients.</p>
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)?	Yes
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 website is hosted on secure government cloud and runs web applications to allow authorized users to log in with credentials to perform tasks related to patient care, such as documenting care in the EMR or accessing telemedicine capabilities.

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?	Yes
PTA - 12A:	Select the type(s) of website measurement and customization technologies in use and if it is used to collect PII.	Persistent Cookies - Does Not 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?	Yes
PTA - 14A:	Is the mobile application HHS developed and managed or a third-party application?	Third-party
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.	The mobile app is designed to be a log-in access point for our medical providers. Only those that have been credentialed into the system have access. Not for the public.
PTA - 16:	Does the mobile application/ have a privacy notice?	Yes
PTA - 17:	Does the mobile application contain links to non-federal government websites external to HHS?	No
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?	No
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?	No
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 Medical records (PHI) Date of Birth Mailing Address Medical Records Number User Credentials Patient ID Number Other - Free text Field - Provider License #
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared.	Business Partners/Contacts (Federal, state, local agencies) Employees/ HHS Direct Contractors Grantees Patients Members of the public Vendors/Suppliers/Third-Party Contractors (Contractors other than 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?	<p>The use of PII within this system is controlled on a need-to-know basis. To document medical treatment, and telemedicine consultations rendered to patients and or animals.</p> <p>To conduct quality assurance reviews and establish a quality improvement process by reviewing medical treatment and consultations on a specific deployment, spotting best practices, and developing process improvements for future deployments.</p> <p>For user authentication and access control.</p>
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research).	There are no secondary uses for PII. The previous entry was in error. Please see comments for verification.
PIA - 6:	Describe the function of the SSN, Truncated SSN, and/or Taxpayer ID.	
PIA - 6A:	Cite the legal authority to use the SSN, Truncated SSN, and/or Taxpayer ID.	
PIA - 7:	Identify legal authorities governing information use and disclosure specific to the system and program.	5 USC 301, Departmental regulations. 5 USC 552a of the Privacy Act of 1974, as amended
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.	<p>Only authorized users with login credentials and access permission per user role are allowed to retrieve record using:</p> <ul style="list-style-type: none"> Patient Name Date of Birth By event and location/site Patient ID number or bar code
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.	<p>09-90-0040 National Disaster Medical System (NDMS) Disaster Medical Information Suite (DMIS)</p> <p>SORN history: 78 FR 78959 (12/27/13), *83 FR 6591 (2/14/18)</p>
PIA - 9:	Identify the sources of PII in the system.	<p>Directly from an individual about whom the information pertains</p> <ul style="list-style-type: none"> In-person Government Sources Other Non-Government Sources Other
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.	N/A
PIA - 11:	Is the PII shared with other organizations outside the system's Operating Division?	Yes
PIA - 11A:	Identify with whom the PII is shared or disclosed.	<ul style="list-style-type: none"> Other Federal Agency/Agencies Private Sector State or Local Agency/Agencies Within HHS
PIA - 11B:	Please provide the purpose(s) for the disclosures described in PIA - 11A.	<p>When engaged by Health and Human Services have access to the records in order to perform</p> <p>patient. Disclosure of a patient's location or status for the life, safety, health, or well-being of the</p> <p>integrity of information maintained in this system</p>

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)).	Business Associate Agreements (BAAs); Data Use Agreement (DUA), Information Sharing Agreement are all complete prior to the release of any information sharing or disclosures.
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.	<p>The BAAs and the DUA are all logged, tracked, and accounted for on a stored secure drive for legal documents with the federal contractor.</p> <p>Requests for disclosure of PII that are received by ASPR Disaster Team (DT) are scanned or saved, logged, tracked, and accounted for on its secure drive. It is organized by date of request and status of request.</p> <p>Information accessed on the system stores the user Identification (ID) and time log for all user that access PII. Those logs are accessible by the DT admin only.</p>
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.	Personally Identifiable Information (PII) are only collected at the time the user accounts are created, and the source of the information is the users themselves, so they have the option to decline the provision of the access, or the services provided by the platform at the time of the account creation.

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.

Individuals seeking to know if ASPR Disaster Telemedicine Platform (ADTP) system contains records about them must submit a written request to the Program Director at the below mailing address or email to, clearly marked as a "Privacy Act Request" on the envelope and letter (see, generally, HHS Privacy Act regulations found at 45 CFR Part 5b). Requests pertaining to patients should include the full name of the patient, appropriate verification of identity, current address of the patient and the name of the requester, appropriate verification of identity, current address of the requester, and the nature of the record sought, as required by HHS Privacy Act regulations at 45 CFR 5b.5. Requests pertaining to owners of animals should include the full name of the owner and the animal, appropriate verification of identity, current address of the requester, and the nature of the record sought, as required by HHS Privacy Act regulations at 45 CFR 5b.5

Disaster Telemedicine Program Director
and Address:

ASPR DT Program Director
400 7th Street, SW Washington D.C.
20024

Or email to asprdt@hhs.gov

Individuals can contact our director or staff duty officer for any privacy concerns. Any concern will be addressed and handled according to policy guidelines by authorized personnel.

Steps that an individual can take if PII is compromised according to HHS breach policy are: Confirm the Breach, Report the Breach, File a HIPAA Complaint with HHS OCR, Protect Yourself from Identity Theft initiating credit monitoring or identity theft protection services.

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.

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.	The ASPR Data Transfer Protocol (DTP) employs file integrity protection to continuously monitor and alert any changes. Unauthorized changes are flagged for investigation by the security team. The Security Team also uses Center for Internet Security (CIS) level 2 and Security Technical Implementation Guides (STIGs) conformance packs to check secure configurations. Alerts are collated and resolved in Asana.
PIA - 17:	Identify who will have access to the PII in the system.	Users Administrators Others
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.	<div style="border: 1px solid black; padding: 10px;"> <p>Clinical Users and Provider – provide create the patient record and have to</p> <p>Non-Clinical site-specific Users are limited data. It just contains general overall</p> <p>Overall Coordinators - limited access high-level operational data.</p> <p>DT Admin which is limited to FTE DT records, etc.</p> </div>
PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Access privileges are controlled through a formal authorization process. The ASPR Disaster Telemedicine Platform applications utilize role-based access control. Only authorized users are permitted access to only that which is expressly required for the performance of their job duties.
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.	<p>The system provides different users different access levels according to their specific role.</p> <p>These are controlled by a menu driven interface in the Clinic Admin Control Panel. The Vice President of Engineering is responsible for ensuring that the application functions are limited to the minimum necessary using menus.</p>

<p>PIA - 21:</p>	<p>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.</p>	<p>The federal contractor mandates security training with KnowBe4 before access to the system for all of their system users. The training covers basic security principles, social engineering risks, supply chain risks, credential protection and remote access risk. This training is updated and documented annually, or when events dictate a revision of content. Those training records are kept in Asana for a minimum of six years. In addition, all contractors must take HHS Records Management Training.</p> <p>ASPR Disaster telemedicine staff, and federal government operators are mandated to annually complete HHS rules of behavior, HHS Records Management, HHS Cybersecurity and privacy awareness trainings.</p>
<p>PIA - 22:</p>	<p>Describe the training system users receive (above and beyond general security and privacy awareness training).</p>	<p>Federal contractor's Security Team sends phishing email information, based on real examples, on how to recognize days of assignment.</p> <p>ASPR Disaster telemedicine staff, and federal government operators are mandated to annually complete HHS rules of behavior, HHS Records Management, HHS Cybersecurity and privacy awareness trainings.</p>
<p>PIA - 23:</p>	<p>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).</p>	<p>Records are retained in accordance with records disposition schedule (NARA) for the Office of Public Health and Emergency Preparedness established the ASPR to serve in a similar capacity as other Medical Records regulated under the Health Information Privacy Act or by any component of HHS/ASPR during a response authority:</p> <p>Cutoff is at the end of the response activity by the Federal Emergency Management Agency Center 2 years after cutoff. Destroy 75 years after cutoff.</p> <p>Cutoff refers to breaking, or ending files at regular intervals into complete blocks and, in this case, cutoff is at the end of the Veterinarian treatment records pertaining to animals. The Veterinarian approves a disposition schedule for them.</p>

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 access requires permission escalation

Connection time outs and requires re-authentication

Full disk encryption is used.

Access is controlled by a set of firewall rules.

Only approved applications are installed on devices.

Internet access is strictly limited to a minimal set of

For physical or logical separation of information flow:
information transfer via shared system resources. Use

Review & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:

Approved

Privacy Analyst Review Date:

5/29/2025

Privacy Analyst Comments:

This was auto-rejected once by Archer. The requested updates have been made to the responses.

Privacy Analyst Days Open:

Moving forward in the review queue to see if auto-rejection occurs again.

Thanks,

Jon

SOP Review

SOP Review Status:

Approved

SOP Signature:

SOP Comments:

2025: PTA 5 states no information sharing but in the PIA it states that information is shared. Please update PTA5, if able to edit. If not, update during the next iteration.

SOP Review Date:

5/30/2025

SOP Days Open: 1

Agency Privacy Analyst Review			
Agency Privacy Analyst Review Status:	Approved	Agency Privacy Analyst Review Date:	6/5/2025
Agency Privacy Analyst Review Comments:	Reviewer: Shanai Shobowale 6/5/2025 All comments were updated. 5/28/2025 Please see comment for PIA-1 and update accordingly. PIA-1: Per PIA-8, Select "Date of Birth".	Agency Privacy Analyst Days Open:	6

SAOP Review			
SAOP Review Status:	Approved	SAOP Signature:	Archer Signature_Bridget Guenther.docx
SAOP Comments:		SAOP Review Date:	6/9/2025
		SAOP Days Open:	4

Supporting Document(s)				
Name	Size	Type	Upload Date	Downloads
No Records Found				

Comments				
Question Name	Submitter	Date	Comment	Attachment
PIA - 9	Data Feed Service, piafrmos_Release	3/20/2025	<p>Directly from an individual about whom the information pertains.</p> <p>In-person</p> <p>Government Sources</p> <p>From medical or clinical personnel treating or evacuating or accessing their personal health record.</p> <p>Federal clinical contractors treating or accessing their personal health record.</p> <p>Non-Government Sources</p> <p>Parent or Guardian</p> <p>Other Family members or individual attending.</p> <p>Owners or caretakers of animals</p> <p>Health Information Exchanges by providers providing direct patient</p>	

care only and info confirmed by patient.

PIA - 11A

Data Feed Service,
piafrmos_Release

3/20/2025

VA, or that participate in
Organizations such as the
bility with HHS for the medical
the purpose of discharging
of health care possible. The
d with relevant partners to
level of health care. The health
alth care operations.
the Congressional office made

tuations arise:

I has agreed to represent the

and, after careful review, the
that the use of such records by
cy collected the records.
performance of a service
perform the activity.

whole or part with federal

e current location and

ie status of the patient.
ief that disclosing such

e information for the purpose
confidentiality of information
ecessary for that assistance.

PIA - 9

Data Feed Service,
piafrmos_Release

5/5/2025

Directly from an individual about
whom the information pertains:

In-person

Government Sources:

From medical or clinical personnel
treating or evacuating or accessing
their personal health record.

Federal clinical contractors treating
or accessing their personal health
record.

Non-Government Sources:

Parent or Guardian

Other Family members or individual attending

Owners or caretakers of animals

Health Information Exchanges by providers providing direct patient care only and info confirmed by patient.

PIA - 1	Data Feed Service, piafrmos_Release	5/7/2025	<p>Please provide a response for the follow question from the general information section: 5: Is the system or electronic information collection agency or contractor operated?</p> <p>Please leave it as an attached comment if you cannot edit the response directly.</p>
PIA - 5	Data Feed Service, piafrmos_Release	5/7/2025	<p>Because you have indicated that the information will be used for research. Please complete the attached Privacy Risk Analysis Checklist. The document can be found in the 'Supporting Documents' section of the PIA near the bottom of the assessment. Please e-mail the completed form to the OS Privacy Inbox when completed.</p>
PIA - 8A	Data Feed Service, piafrmos_Release	5/7/2025	<p>Please remove the bullet points from the response as they are not 508 compliant, switch to a list such as: 'Patient Name, Date of Birth, By event and location/site, Patient ID number or bar code'</p>
PIA - 11B	Data Feed Service, piafrmos_Release	5/7/2025	<p>Please remove the bullet points from the response as they are not 508 compliant.</p>
PIA - 11C	Data Feed Service, piafrmos_Release	5/7/2025	<p>Please remove the bullet points from the response as they are not 508 compliant.</p>
PIA - 18	Data Feed Service, piafrmos_Release	5/7/2025	<p>Please remove the bullet points from the response as they are not 508 compliant.</p> <p>The following can be removed from the bottom of the response: "If "Contractor" is selected, PIA-17A and PIA-17B should populate and be</p>

completed.

If "Contractor" is not selected, complete and move to PIA-18."

PIA - 21	Data Feed Service, piafrmos_Release	5/7/2025	Please remove the bullet points from the response as they are not 508 compliant.
PIA - 22	Data Feed Service, piafrmos_Release	5/7/2025	Please remove the bullet points from the response as they are not 508 compliant.
PIA - 24	Data Feed Service, piafrmos_Release	5/7/2025	Please remove the bullet points from the response as they are not 508 compliant.
PIA - 10C	Data Feed Service, piafrmos_Release	5/7/2025	This response can be changed to 'N/A'.
PIA - 5	Data Feed Service, piafrmos_Release	5/12/2025	<p>Hi, Abigail,</p> <p>We will absolutely NOT use PII in the system for training, testing nor research. That was checked in error. Can you correct for us or how should we correct this error?</p> <p>Sorry for the confusion.</p> <p>Very Respectfully,</p> <p>Christopher Crabtree, DrPH, CEM[®], FAC-COR III, CHEP, CEDP Senior Emergency Management Specialist Project Officer - Pediatric Disaster Care Program Disaster Telemedicine Division Office of International Operations (OIO) Center for Response (CFR) Administration for Strategic Preparedness and Response (ASPR)</p>
PIA - 11C	Data Feed Service, piafrmos_Release	5/15/2025	Please update to use present tone. The PIA should be completed as if the system is live today.
PIA - 15	Data Feed Service, piafrmos_Release	5/15/2025	What is the process? Can you provide a brief summary of the process that

is outlined in the policy?

PIA - 11C	Data Feed Service, piafrmos_Release	5/15/2025	The response cannot be changed but below is the edited response: Business Associate Agreements (BAAs); Data Use Agreement (DUA), Information Sharing Agreement are all complete prior to the release of any information sharing or disclosures.
PIA - 15	Data Feed Service, piafrmos_Release	5/15/2025	The original response cannot be altered but the update is below: Steps that an individual can take if PII is compromised according to HHS breach policy are: Confirm the Breach, Report the Breach, File a HIPAA Complaint with HHS OCR, Protect Yourself from Identity Theft initiating credit monitoring or identity theft protection services.
PIA - 1	BLAND, CRYSTAL	5/28/2025	5/28/2025 On the next iteration of the PTA please list the PII listed in PIA-1 in PTA-5 (i.e. name, date of birth, patient Id#, and Providers License#).
PIA - 1	BLAND, CRYSTAL	5/28/2025	5/28/2025 Per PIA-8, Select "Date of Birth".

Admin Section

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

Miscellaneous Fields

Last Updated:	6/9/2025 1:36 PM	History Log:	View History Log
---------------	------------------	--------------	----------------------------------