PTA / PIA: HRSA - LERD - QTR3 - 2025 - HRSA1446281

Created Date: 8/25/2025 12:21 PM Last Updated: 8/29/2025 4:21 PM

General Information

PTA / PIA Name:	HRSA - LERD - QTR3 - 2025 - HRSA1446281	**PTA / PIA ID:**	3706356
Component Name:	HRSA - Labor and Employee Relations Database	**ATO Boundary Name:**	Labor and Employee Relations Database
Overall Status:	Complete	**# of Days - Open:**	49
Submitter:		**Submit Date:**	7/11/2025
Next Assessment Date:	N/A	**Expiration Date:**	1/1/2100
Office:		**OpDiv:**	HRSA
Security Categorization:	Moderate		
Make PIA available to Public?:	No	**PIA Required:**	Yes

General 01:	Identify the Enterprise Performance Lifecycle Phase of the system.	Operations and Maintenance
General 02:	Is this a FISMA-Reportable system?	Yes
General 03:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	Yes
General 04:	ATO Date or Planned ATO Date.	3/15/2024
General 05:	Is the system or electronic information collection, agency or contractor operated?	Contractor
History Log:	View History Log	

Privacy Threshold Analysis

Privacy Threshold Analysis

PTA 01:	Point of Contact (POC) Name	Rebecca Andam Michael Makinde
PTA 01A:	POC Title and Organization	ISSO, HRSA
PTA 01B:	POC Email Address	RAndam@hrsa.gov
PTA 01C:	POC Phone Number	301-370-9562
PTA 02:	Indicate the following reason(s) for this PTA. Choose from the following options.	PIA Validation (PIA Refresh)
PTA 02A:	Describe in further detail any changes to the system that have occurred since the last PIA.	No changes since last PTA

PTA 03:	Is the data contained in the system owned by the agency or contractor?	Agency
PTA 04:	Please give a brief overview of the purpose of the system by describing what the functions of the system are and how the system carries out those functions in support of HHS.	To improve personnel management operations, the Labor and Employee Relations Database (LERD) application is a database designed to collect and store information about all Labor Employees Records (LER) actions in one system that allows for faster and more reliable data retrieval and reporting. System features include custom views to allow the LER staff to review case status information, run scanned and ad-hoc reports.
PTA 05:	List and/or describe all the types of information that are collected, maintained, and/or shared by the system regardless of whether that information is PII and how long that information is stored.	LERD is a database case management system that collects and stores information about all Labor Employees Records (LER) actions in one system. The type of information the system collects, maintains (store), or share are information about the employee; name, e-mail address, employment status, pay plan, pay scale, job series, Position title, grade, and Bargaining Unit Status. The system also maintains details about employee grievances, complaints, legal suits, corrective actions, and other Human Resources complaints. At times cases relate to an employees medical condition and therefore requiring the HR specialist to upload medical documentation related to the case to the system. Information about the case is collected outside of this system by HRSA's Human Relations Labor and Employee Relations specialist. The specialist then logs into the LERD application using their government issued PIV card. Once in the system the specialist records the date when information was received, when additional information is expected, and uploads any documentation collected. The LERD application is only accessible within the HRSA network and not accessible from the outside. Only HRSA's Labor and Employee Relation specialist and HRSA's Office of Information Technology have access to the application. At this time, no contractors have access to the production data or environment. For the system users, the system records their first and last name, logon ID, and system role.
PTA 05A:	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.
PTA 05C:	Please identify the system that maintains the user credentials or controls access to this system.	HRSA AMS and HRSA AD

PTA 06:	Describe why each type of information is collected, maintained, and/or shared by the system. Specify what information is collected about each category of individual.	Labor and Employee Relations (LER) department record employee related grievances and outcomes. Prior to LERD, the HR specialist tracked employee related issues using spreadsheets. LERD allows multiple specialist to review the data, return to the data to update and reports to be generated. Specifically, LERD collects the following data related to the employee employee; name, e-mail address, employment status, pay plan, pay scale, job series, Position title, grade, and Bargaining Unit Status. When a case is brought to the attention of the Labor and Employee Relations team, they begin building the case in the LERD application. First information is entered on a high level; Initial Contact Date, Initial Consult Date, and LER Specialist Assigned to Case. Next the specialist will add details to the case. They begin by entering notes about the documents that the specialist collected outside of the system. Then the specialist records the date which they asked for the documentation, when the documentation was received, when the documentation was reviewed, and finally when a response was given. In the case where a legal trial is needed, additional information is collected; when documents where submitted to the attorneys, dates of any mediation, date of the court hearing, and any outcome from those hearings. The LERD application also allows for the LER specialist to record the time a Union Representative spends resolving a dispute, negotiating union terms, and time spent in meetings and/or training. These numbers are then used for end of the year reports.
PTA 07:	Does the system collect, maintain, use, or share PII?	Yes
PTA 08:	Does the system include a website or online application?	Yes
PTA 08A:	Provide the URL(s).	Production: https://lerd.hrsa.gov QA: https://lerdqa.hrsa.gov Dev: https://lerddev.hrsa.gov
PTA 08B:	Are any of the website or online applications accessible by the public (including publicly accessible log in pages)?	No
PTA 09:	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 purpose of LERD is to store about all Labor Employees Records (LER) actions in one system. Access to LERD is role based and the access is granted by the system owner after coordination with business owner about the role to be assigned to the users and the website logins are managed by HACAP/AMS authentication
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 12:	Does the website use web measurement and customization technology?	No
PTA 13:	Does the website have any information or pages directed at children under the age of thirteen?	No
PTA 14:	Does the system have a mobile application?	No
PTA 20:	Are any third-party websites or applications (TPWA) associated with the system?	No
PTA 21:	Does this system use artificial intelligence (AI) tools or technologies?	No

Privacy Impact Assessment

Privacy Impact Assessment

PIA 22:	Indicate the type(s) of personally identifiable information (PII) that the system will collect, maintain, or share.	Biographical Information Name Employment Status/History Contact Information Email Address (Business) Other Other
PIA 22A:	Identify the “other” type(s) of personally identifiable information (PII) not mentioned in the above list.	Free text Field: Grade, Position Title, pay plan, pay scale, job series, position title, grade, bargain unit status, grievances, legal suits, and HR complaints.
PIA 23:	Indicate the categories of individuals about whom PII is collected, maintained, or shared.	Employees/HHS Direct Contractors
PIA 24:	Indicate the approximate number of individuals whose PII is maintained in the system.	500 – 4,999
PIA 25:	For what primary purpose is the PII used?	The primary purpose for using the Employee's Name is to organize data. Email address is used to verify information is entered for the correct employee.
PIA 26:	Describe any secondary uses for which the PII will be used (e.g., testing, training, or research).	There is no intended secondary use for PII data.
PIA 28:	Identify legal authorities, governing information use and disclosure specific to the system and program.	Disciplinary, Adverse (5 CFR 752), and Performance-Based Actions (5 CFR 432) Case Files. Records and tracking database related to disciplinary, adverse, and performance-based actions taken against employees. Also included are separate employee-specific files documenting actual and attempted inappropriate use of National Archives and Records Administration (NARA) office equipment
PIA 29:	Are records in the system retrieved by one or more PII data elements?	Yes
PIA 29A:	Please specify which PII data elements are used to retrieve records.	Name

PIA 29B:	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 09-90-0018, Personnel Records in Operating Offices, HHS/OS/ASPER
PIA 30:	Identify the sources of PII in the system.	Government Sources Within the OPDIV
PIA 31:	Is there an Office of Management and Budget (OMB) information collection approval number?	No
PIA 31B:	Explain why an OMB information collection approval number is not required.	The system does not collect information because it is subject to the Paperwork Reduction Act.
PIA 32:	Is the PII in the system shared directly with other organizations outside the system's Operating Division?	No
PIA 33:	Is the submission of PII by individuals voluntary or mandatory as defined in the Privacy Act?	Voluntary
PIA 34:	Describe the method in place to notify and obtain consent from individuals whose PII will be collected. If no prior notice is given or consent cannot be obtained, explain why.	Individuals are informed when they submit the information that will be stored in the system that it will be used for legitimate purposes to avoid conflict of interest. No other notification or consent beyond this is required.
PIA 35:	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). If they cannot be notified or have their consent obtained, explain why.	Individuals are informed when they submit the information that will be stored in the system that it will be used for legitimate purposes to avoid conflict of interest. No other notification or consent beyond this is required.
PIA 36:	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 individual would contact the Labor and Employee Relations (LER) team through Human Resources. Once the inquiry is received by the LER team. The LER team would address the matter accordingly.
PIA 37:	Describe the process in place for periodic reviews of the system to ensure the integrity, availability, accuracy, and relevancy of the PII in the system. Please address each element in your response. If no processes are in place, explain why not.	Annual reviews are carried out, and updates are applied (if necessary) to maintain the integrity, availability, accuracy, and relevancy of the data.
PIA 38:	Identify who will have access to the PII in the system.	Users Administrators
PIA 39:	Provide the reason why each of the groups identified in 38 needs access to PII.	Users: Users access LERD as part of their daily job, users will look up information in the LERD system by employee's name. Administrators: Office of Information Technology (OIT) administrators of the system will have access to the database which stores the PII to ensure the system is running correctly.
PIA 40:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Access to PII is granted by the System Owner who determines which users within an organization should be granted access to PII contained within the application.

PIA 41:	Describe the technical methods in place to allow those with access to PII to access only the minimum amount of information necessary to perform their job.	Access to data that exists in the system is only granted to users by the system owner. There are specific roles defined in the system and each role has access only to data that it is granted access to. Users must enter a correct username and password to enter the system.
PIA 42:	Identify the general security and privacy awareness training provided to system users (system owners, managers, operators, contractors and/or program managers) to make them aware of their responsibilities for protecting the information being collected and maintained.	All users have completed IT Security Awareness and Records Management Training.
PIA 43:	Describe the training system users receive above and beyond general security and privacy awareness training.	NA
PIA 44:	Describe the process and guidelines in place for the retention and destruction of PII. Cite specific National Archives and Records Administration (NARA) records retention schedule(s) and include the retention period(s).	National Archives and Records Administration (NARA) General Records Schedule 2.5 - records automatically deleted after 6 years.
PIA 45:	Describe how the PII will be secured in the system using administrative, technical, and physical controls. Please address each element in your response.	LERD relies on network security controls provided by HRSA managed through General Support System (GSS). The LERD implements firewalls, network and host based intrusion detection to secure its facilities. Boundary entry points are controlled by firewall rules and protected by Intrusion Detection Servers to prevent unauthorized access. System security compliance is maintained by patching regularly. Client server communication is encrypted by SSL. Data at rest is encrypted. System access and usage is frequently audited.

Review and Comments

OpDiv Privacy Analyst Review

Privacy Analyst Review Decision:	Approved	**Privacy Analyst Review Date:**	7/25/2025
Privacy Analyst Review Comments:		**# of Days - PA Review:**	14

SOP Review

SOP Review Decision:	Approved	**SOP Review Date:**	8/25/2025
SOP Review Comments:		**# of Days - SOP Review:**	31

Agency Privacy Analyst Review

Agency Privacy Analyst Review Decision:	Approved	**Agency Privacy Analyst Review Date:**	8/28/2025
Agency Privacy Analyst Review Comments:	Reviewer: Crystal Bland 8/28/2025 This PIA is ready for SAOP review and approval.	**# of Days - APA Review:**	3

SAOP Review

SAOP Review Decision:	Approved	**SAOP Review Date:**	8/29/2025
SAOP Review Comments:		**# of Days - SAOP Review:**	1

SAOP Signature

Date	User	Type	Name	Original Value	New Value
8/29/2025 1:39 PM	BAUR, VANESSA	Signature	SAOP (Email PIN)		Content Signed

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
No Records Found				

Comments

Question Name	Submitter	Date	Comment	Attachment
No Records Found				