**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 ID     | 1439654 |
|------------|---------|---------|
| PIA Name   | HRSA - PAPM - QTR1 - 2022 - HRSA794758 |
| OpDiv      | HRSA |

**PTA**

<table>
<thead>
<tr>
<th>PTA - 1A: Identify the Enterprise Performance Lifecycle Phase of the system</th>
<th>Operations and Maintenance</th>
</tr>
</thead>
<tbody>
<tr>
<td>PTA - 1B: Is this a FISMA-Reportable system?</td>
<td>Yes</td>
</tr>
<tr>
<td>PTA - 2: Does the system include a website or online application?</td>
<td>No</td>
</tr>
<tr>
<td>PTA - 3: Is the system or electronic collection, agency or contractor operated?</td>
<td>Agency</td>
</tr>
<tr>
<td>PTA - 3A: Is the data contained in the system owned by the agency or contractor?</td>
<td>Agency</td>
</tr>
<tr>
<td>PTA - 5: Does the system have or is it covered by a Security Authorization to Operate (ATO)?</td>
<td>Yes</td>
</tr>
<tr>
<td>PTA - 5A: If yes, Date of Authorization</td>
<td>11/15/2019</td>
</tr>
<tr>
<td>PTA - 6: Indicate the following reason(s) for this PTA. Choose from the following options.</td>
<td>PIA Validation (PIA Refresh)</td>
</tr>
<tr>
<td>PTA - 7: Describe in further detail any changes to the system that have occurred since the last PIA</td>
<td>There have been no changes to the system since the last PIA</td>
</tr>
<tr>
<td>PTA - 8: 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?</td>
<td>Personnel Action and Payroll Management system (PAPM) provides, in a single location, personnel and payroll information drawn directly</td>
</tr>
</tbody>
</table>
from the official systems of record for both Commissioned Corps (CC) and Civil Service (CS) employees. Systems of record include the Business Intelligence Information System (BIIS) and the Accounting For Pay System (AFPS), both of which have their own Privacy Impact Assessments. On the personnel, or Full Time Equivalent (FTE), side, some important elements are equal employment opportunity (EEO) information such as pay plan, grade, series, step, position title, employment status, education record, administrative code, common accounting number (CAN), and regular and overtime hours worked by the employee. On the payroll side, several data elements are available, including pay date, gross pay, net pay, gross expenditures, and pay period. The system generates year-to-date payroll information monthly and quarterly, as requested by the user. Timeliness is ensured through regular extracts from time-attendance and payroll servers; the extracts are timed with the running of the official payroll programs.

**PIA**

**PIA - 1:** Indicate the type of PII that the system will collect or maintain

- Social Security Number
- Name
- E-Mail Address
- Phone numbers
- Education Records
- Military Status
- Date of Birth
- Employment Status

**PIA - 2:** Indicate the categories of individuals about whom PII is collected, maintained or shared

- Employees/ HHS Direct Contractors

**PIA - 3:** Indicate the approximate number of individuals whose PII is maintained in the system

- Above 2000

**PTA - 9:** 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.

- Name SSN
- Date of Birth Position Title Grade and Series Pay plan Education Records Salary Military Status Employment Status Administrative code Common accounting number Username Payroll data FTE hour data

**PTA - 9A:** Are user credentials used to access the system?

- Yes

**PTA - 9B:** Please identify the type of user credentials used to access the system.

- HHS User Credentials
- HHS/OpDiv PIV Card

**PTA - 10A:** Are records in the system retrieved by one or more PII data elements?

- Yes

**PTA - 10B:** Please specify which PII data elements are used.

- Name, Phone Number, Social Security Number, Address

**PTA - 11:** Does the system collect, maintain, use or share PII?

- Yes
**PIA - 4:** For what primary purpose is the PII used?  
Personnel Action and Payroll Management (PAPM) users in the Office of Budget (OB) use PII to identify employees, research their employee status and personnel actions, and apply changes to their projected payroll and Full time employee (FTE) hours. HRSA Bureaus review and edit worksheets with employee PII within the PAPM system and check for accuracy of data. The Bureau Analysts are only able to view and edit data specific to their own Bureau. User credentials are collected to control who can access the system. PAPM does not have application-level user credentials, and relies on HRSA network user credentials instead.

**PIA - 5:** Describe any secondary uses for which the PII will be used (e.g. testing, training or research)  
PAPM will not use PII for testing and training.

**PIA - 6:** Describe the function of the SSN/Taxpayer ID.  
PAPM extracts data from different systems, and because the format of the employee name is different in each source system, the only common factor for identifying employees is the SSN. Therefore, PAPM uses the SSN to maintain employee records of payroll and FTE data. There may also be multiple employees with the same name, in which case the SSN is used to identify each employee.

**PIA - 6A:** Cite the legal authority to use the SSN  
Chief Financial Officer Act of 1990  
E-Government Act of 2002

**PIA - 7:** Identify legal authorities, governing information use and disclosure specific to the system and program  
Chief Financial Officer Act of 1990  
Privacy Act of 1974  
Federal Information Security Management Act of 2002  
19 CFR 163 Record Keeping of Sensitive Data  
OMB Memoranda M-99-20  
OMB Circular A-123 and A-130  
NIST SP 800-14

**PIA - 8:** 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.  
09-90-0020 Suitability for Employment Records SORN history: 58 FR 28880 (5/17/93); updated 59 FR 55845 (11/9/94), *83 FR 6591 (2/14/18) [Exempt based on (k)(5); see 40 FR 47406 & 40 FR 41140]

**PIA - 9:** Identify the sources of PII in the system  
Government Sources  
Within the OPDIV  
Other HHS OPDIV

**PIA - 9A:** Identify the OMB information collection approval number or explain why it is not applicable.  
PAPM does not require an OMB approval number.

**PIA - 10:** Is the PII shared with other organizations outside the system's Operating Division?  
No

**PIA - 11:** 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 publication of a Systems of Records Notice in the Federal Register notifies individuals that their personal information will be collected.

**PIA - 12:** Is the submission of PII by individuals voluntary or mandatory?  
Voluntary
| PIA - 13: | 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. | There is no process in place to for individuals to opt-out of the collection of their personal information. PAPM is a reporting system that extracts existing data containing PII from the HHS Human Resource Office. |
| 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. | There is no process in place to notify individuals of their consent for use of their PII when major changes occur to the system. The collection of their personal information is extracted from the HHS Human Resource Office and imported into PAPM for Payroll reports. Information is collected by Human Resource office when people are hired. |
| 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 can contact the HRSA Human Resource Office if they have concerns about their PII. |
| PIA - 16: | Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy. Please address each element in your response. If no processes are in place, explain why not. | The accuracy of the PII entered into the Human Resource (HR) is validated during the data entry process outside of the PAPM application. PAPM received data from the HR system. PAPM continually validates the integrity, accuracy, availability, and relevancy of the PII received and verified during these quality audits. |
| PIA - 17: | Identify who will have access to the PII in the system and the reason why they require access. | Users |
| PIA - 17A: | Provide the reason of access for each of the groups identified in PIA -17. | Developers |
| PIA - 17B: | Select the type of contractor. | Contractors |
| PIA - 18: | Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII. | PAPM is a role-based application. Access to PII is determined by the system owners and what functions are necessary to perform user tasks. |
| PIA - 19: | 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. | PAPM restricts user access based on roles and privileges pertaining to each specific Bureau. |
| PIA - 20: | 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. | PAPM users are required to take the HRSA IT General User’s Security, and Privacy yearly training. |
| PIA - 23: | Describe the process and guidelines in place with regard to the retention and destruction of PII. Cite specific NARA records retention schedule(s) and include the retention period(s). | National Archives and Records Administration (NARA) General Records Schedule 25 - records automatically deleted after 6 years. HRSA |
General Support Systems (GSS) is responsible for this activity. The storage, handling, and destruction of PAPM media is the responsibility of HRSA Office of Information Technology (OIT) and is covered in the June 2003 HRSA OIT GSS Local Area Network System Security Plan. A procedure for marking PAPM reports, such as —"Time Sensitive Information Subject to Change," “Limited Official Use,” —is currently in place. General Schedule 21.A and General Schedule 20 Item 12A.

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

The security of the system falls under HRSA General Support Services (GSS), which abides by all rules and regulations regarding system security and integrity, vulnerability scanning, data storage and backup, and data encryption. Access to the system is only permitted within the HRSA network, which is controlled by GSS through the use of Personal Identity Verification (PIV) cards. However, only approved user accounts are allowed access to the system. PAPM user accounts must be approved by the user's bureau supervisor and the PAPM Information System Security Officer (ISSO). Additionally, PAPM users must agree and adhere to the PAPM Rules of Behavior before being granted system access.