PTA / PIA: HRSA - IntegrityM - QTR1 - 2026 - HRSA1464460

Created Date: 3/3/2026 11:21 AM Last Updated: 5/29/2026 4:02 PM

General Information

PTA / PIA Name:	HRSA - IntegrityM - QTR1 - 2026 - HRSA1464460	**PTA / PIA ID:**	4316208
Component Name:	HRSA - IntegrityM	**ATO Boundary Name:**	IntegrityM
Overall Status:	Complete	**# of Days - Open:**	141
Submitter:		**Submit Date:**	5/14/2026
Next Assessment Date:	05/28/2029	**Expiration Date:**	5/28/2029
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.	10/13/2023
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	Tibor Molnar
PTA 01A:	POC Title and Organization	IntegrityM IT Manager
PTA 01B:	POC Email Address	tmolnar@integritym.com
PTA 01C:	POC Phone Number	703-236-1275
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 have occurred
PTA 03:	Is the data contained in the system owned by the agency or contractor?	Contractor

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.	The Children's Hospitals Graduate Medical Education (CHGME) Program and the Teaching Health Center Graduate Medical Education (THCGME) Program provide federal funding to support medical and dental residency training. Because participating children's hospitals and teaching health centers oversee large numbers of residency programs and trainees, the contractor is responsible for assessing full-time equivalent (FTE) resident counts and reviewing supporting documentation for all applicable cost-reporting periods, as required under Section 1886 of the Social Security Act. The assessment system is designed to securely collect, store, and manage information to ensure compliance with federal regulations, policies, and program guidelines when determining which residents qualify for GME funding. The finalized FTE assessments will be available to the Centers for Medicare & Medicaid Services (CMS) auditors and will be used to verify the accuracy of FTE counts included in or excluded from Medicare Cost Reports, depending on whether the institution receives CMS funding and whether training occurred in CHGME or THCGME settings.
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.	The system will contain information obtained from the children's hospitals and teaching health centers participating in the CHGME and THCGME programs. This will include FTE resident counts and additional supporting documentation provided by the providers and MACs for all relevant cost report periods. The system will also contain Personally Identifiable Information (PII) including: SSN, Name, DOB, email address, phone number, graduate certificate, education records, legal documents and employment status. This data is stored/archived based on federal record storage requirements.
PTA 05A:	Are user credentials used to access the system?	Yes
PTA 05B:	Please identify the type of user credentials used to access the system.	HHS User Credentials HHS/OpDiv PIV Card HHS Email Address HHS Username Password Non-HHS User Credentials Username Password

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.	For audit and HRSA reporting purposes, data is collected from both providers and Medicare Administrative Contractors (MACs). **Provider-submitted information includes:** • Complete lists of all interns and residents reported on the HRSA 99-1 and the Medicare cost report • Resident rotation schedules and code definitions • Written agreements with non-hospital training sites • Lists of part-time residents • Lists of residents in non-approved programs, CRNA replacement positions, and moonlighting roles • Documentation for residents training in nonprovider settings • ECFMG certificates for international medical graduates • All affiliation agreements and addendums • CVs/files for dental and podiatry residents, when applicable • graduate certificate **MAC-submitted information includes:** • CMS Star screen showing Medicare Cost Report status • IRIS electronic files • Medicare Worksheet E-4 • GME base year cap affiliation agreements and related correspondence
PTA 07:	Does the system collect, maintain, use, or share PII?	Yes
PTA 08:	Does the system include a website or online application?	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.	Identifying Numbers Social Security Number Biographical Information Name Date of Birth Certificates (e.g., training certificates) Education Records Employment Status/History Legal Documents Contact Information Email Address (Personal) Phone Numbers (Personal) Email Address (Business) Phone Numbers (Business)
PIA 23:	Indicate the categories of individuals about whom PII is collected, maintained, or shared.	Grantees
PIA 24:	Indicate the approximate number of individuals whose PII is maintained in the system.	5,000 – 9,999
PIA 25:	For what primary purpose is the PII used?	To fulfill the requirements of HRSA's FTE GME Resident Assessment contract, ensuring financial and operational compliance with CMS and HRSA GME.
PIA 26:	Describe any secondary uses for which the PII will be used (e.g., testing, training, or research).	N/A
PIA 27:	Describe the function of the SSN, Truncated SSN, and/or Taxpayer ID. If the Taxpayer IDs collected are only for businesses include that in your response.	As required by the HRSA contract to properly identify interns and residents.
PIA 27A:	Cite the legal authority to use the SSN, Truncated SSN, and/or Taxpayer ID. If the Taxpayer IDs collected are only for businesses, you may respond N/A.	2 CFR 200-oversight monitoring for grants per the HRSA FTE GME contract
PIA 28:	Identify legal authorities, governing information use and disclosure specific to the system and program.	HRSA and CMS
PIA 29:	Are records in the system retrieved by one or more PII data elements?	No
PIA 30:	Identify the sources of PII in the system.	Government Sources Within the OPDIV Non-Government Sources Private Sector
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.	N/A contractor owned vendor system
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.	HRSA notifies program participants via emails and webinars of the documents and data to be collected as part of the annual FTE GME Assessment – per the requirements of 2 CFR 200 and HRSA/CMS Policy. Consent is not 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.	Consent is not required because the collection of PII is mandated under federal law and regulatory requirements associated with administering federal grants. 2 CFR 200
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.	Individuals who believe their personally identifiable information (PII) has been improperly collected, used, disclosed, or recorded inaccurately will follow IntegrityM's policy for incident reporting. If misuse or unauthorized disclosure is confirmed, corrective actions are taken immediately—such as limiting access, updating safeguards, or notifying federal partners if required. If the issue involves inaccurate PII, the information is corrected and verified. The individual receives a written response summarizing the findings and any actions taken. All complaints and resolutions are documented and used to improve training, controls, and internal processes to ensure ongoing compliance with 2 CFR 200 requirements for safeguarding PII.
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.	Leveraging IntegrityM's formal security plan, privacy policies, and the data security requirements established under our HRSA contract, IntegrityM conducts scheduled internal audits, data validation procedures, and systematic access reviews. These controls ensure that all PII housed within the system remains accurate, reliable, relevant, secure, and readily accessible. This comprehensive approach fully supports federal grant oversight responsibilities and maintains continuous compliance with 2 CFR 200.
PIA 38:	Identify who will have access to the PII in the system.	Contractors
PIA 38A:	Select the type of contractor.	HHS/OpDiv Direct Contractors
PIA 38B:	Do contracts include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices?	Yes
PIA 39:	Provide the reason why each of the groups identified in 38 needs access to PII.	To perform the requirements of the HRSA FTE GME Contract
PIA 40:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	IntegrityM user controls and access policy
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.	User names/passwords required in addition to federal security clearance to access contract data. Access and user control policies, access audits. Auditors are only provided access to the providers/data for which they are assigned.

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.	Annual IntegrityM Privacy and security training and HRSA Privacy and security training.
PIA 43:	Describe the training system users receive above and beyond general security and privacy awareness training.	Compliance training, Conflict of Interest,
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).	IntegrityM manages Federal Personally Identifiable Information (PII) in accordance with **2 CFR 200.334 (Retention Requirements for Records)**, applicable federal privacy laws, HRSA contractual requirements, and the **National Archives and Records Administration (NARA)** records retention schedules. These requirements ensure that all PII is retained only for the period necessary to meet federal oversight, audit, and programmatic needs, and then destroyed securely to prevent unauthorized disclosure. The NARA General Records Schedule (GRS) 1.1
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.	**Administrative Controls** 1. Access to sensitive information, including PII and contract data, is limited to authorized personnel based on business need and role-based authorization. 2. User access rights are assigned according to the principle of least privilege and need-to-know requirements. 3. Shared, guest, anonymous, temporary, vendor, and service accounts are prohibited. 4. Unique usernames and passwords are required for each authorized user account. 5. All accounts are approved and managed by IntegrityM IT System Administrators. 6. Project managers and system owners authorize access requests through formal ticketing and approval processes. 7. Human Resources coordinates with IT Operations to ensure terminated or transitioned staff accounts are promptly disabled and credentials revoked. 8. User accounts are reviewed periodically, and inactive accounts are disabled in accordance with established retention and inactivity thresholds. 9. Privileged access is restricted to authorized IT Operations personnel only. 10. Administrative and functional duties are separated to reduce conflicts of interest and enforce segregation of duties. 11. IntegrityM maintains formal policies governing data access, information security, remote use, separation of duties, and account management. 12. Security policies and procedures are reviewed annually and updated as necessary. 13. Security policies and procedures are disseminated to management, operations staff, and executive leadership.

14. Remote work involving sensitive information is restricted to authorized users and governed by secure remote access requirements.
15. Employees are required to sign remote use and acceptable use authorization agreements upon hire and annually.
16. IT Operations staff monitor user account activity and privileged actions for suspicious or atypical behavior.
17. Security incidents, high-risk user actions, and unauthorized activities are reviewed and escalated through established incident response procedures.
18. IntegrityM enforces formal onboarding, account provisioning, transition, and offboarding procedures.
19. Access to project folders, mapped drives, and applications is restricted based on assigned roles and operational responsibilities.
20. IntegrityM maintains audit logging, user activity monitoring, and periodic access reviews to ensure accountability and compliance.

Technical Controls

1. Contract data and sensitive information are encrypted using FIPS 140-2 validated encryption technologies.
2. Laptop hard drives are encrypted using PGP Desktop validated to FIPS 140-2 standards.
3. Server hard drives utilize hardware-based encryption validated to FIPS 140-2 standards.
4. Data at rest is encrypted using approved encryption technologies.
5. Remote access connections utilize secure VPN encryption.
6. VPN sessions automatically disconnect after periods of inactivity.
7. Multi-factor authentication and secure authentication controls are implemented for remote access and privileged access activities.
8. Unique user credentials are required for all system authentication.
9. IntegrityM employs role-based access controls and logical segregation of contract data and project resources.
10. Firewalls and intrusion detection systems are implemented to prevent unauthorized information flow and detect malicious activity.
11. Automated logging and monitoring solutions track user activity, account changes, authentication events, and privileged actions.
12. Automated alerts notify IT personnel of suspicious or high-risk activities.
13. Windows event logs and Active Directory logs are centrally monitored and retained for audit purposes.
14. Audit logging systems are used to inspect

unauthorized access attempts, privileged functions, and system activities.
15. IntegrityM uses centralized log management and reporting tools to support continuous monitoring.
16. Only authorized IT Operations personnel may install, configure, or update software on IntegrityM systems.
17. Non-privileged users are restricted from executing administrative or security-altering functions.
18. Access management activities including account creation, modification, disabling, and removal are monitored and logged.
19. Automated inactivity reporting is used to identify and disable inactive accounts.
20. IntegrityM utilizes secure ticketing and workflow systems to manage access provisioning and review processes.

Physical Controls

1. Servers are maintained within physically secure server room environments.
2. Physical access to servers and networking equipment is restricted to authorized personnel only.
3. Office and server room access are controlled using locks, key cards, and restricted entry procedures.
4. Laptops and portable devices containing sensitive information must be secured in locked cabinets or drawers when not in use.
5. Physical access to facilities and systems is limited to personnel with approved business need.
6. IntegrityM maintains safeguards to prevent unauthorized physical access to systems containing sensitive information.
7. Administrative offices and IT infrastructure areas are protected through controlled access mechanisms and physical security procedures.

Compliance Alignment Statement

These safeguards align with federal internal control and cybersecurity requirements, including:

- 2 CFR 200.303 internal control requirements
- NIST SP 800-series cybersecurity and access control guidance
- HRSA contractual data security and privacy requirements
- IntegrityM internal privacy, information security, and cybersecurity policies

Review and Comments

OpDiv Privacy Analyst Review

Privacy Analyst Review Decision:	Approved	**Privacy Analyst Review Date:**	5/18/2026
Privacy Analyst Review Comments:	Please review the answer for PIA-29B - if HRSA owns & manages the SORN, then there should be a SORN number.	**# of Days - PA Review:**	4

SOP Review

SOP Review Decision:	Approved	**SOP Review Date:**	5/18/2026
SOP Review Comments:	5/18/2026 - Reviewed PIA-45 response	**# of Days - SOP Review:**	0

Agency Privacy Analyst Review

Agency Privacy Analyst Review Decision:	Approved	**Agency Privacy Analyst Review Date:**	5/18/2026
Agency Privacy Analyst Review Comments:	Reviewer: Godisgreat Peters 5/18/2026 All comments addressed. This PIA is ready for SAOP review and approval. 5/13/2026 Please see comment and update accordingly: PIA-45: Please list what the Administrative, Technical, and Physical controls are, for example you could say: "**Administrative Controls** Access to PII is limited to **authorized personnel only** User access rights are assigned based on authorization Unique usernames and passwords are required for each authorized user Remote work involving PII is restricted to authorized users and governed through secure access requirements **Technical Controls** Contract data is encrypted using **FIPS 140-2 compliant encryption** Remote access uses a **secure encrypted connection** **Two-factor authentication (2FA)** is required for remote access Unique user credentials (usernames and	**# of Days - APA Review:**	0

passwords) are used for system authentication

Contract data is logically segregated on the server

Physical Controls

Servers are located in a **physically secure server room**

The server room is located at the IntegrityM main office

Office access is controlled using **electronic key cards**

Server room access is restricted by **lock and key**

Physical access to the server room is limited to authorized personnel only.

These safeguards align with federal internal control requirements outlined in **2 CFR 200.303**, NIST SP 800-series guidelines, HRSA's contractual data security requirements, and IntegrityM's internal privacy and cybersecurity policies."

3/3/2026 Please see comments and update accordingly:

PTA-6: Per PTA-5, please include the following PII in your response "graduate certificate."

PIA-22: Per PTA-5, please include the following PII in your response "graduate certificate."

PIA-27A: Please change the word oversite to oversight.

PIA-33: Does refusal to submit PII lead to civil or criminal penalty? If no, please select voluntary.

PIA-42: Please spell out PS.

PIA-43: Please spell out COI.

PIA-44: Please include NARA General Records Schedule (GRS) 1.1, which coincides and aligns with 2 CFR 200.334 standards for financial management records.

PIA-45: Please provide details on how the PII will be secured in the system using administrative, technical, and physical controls. Please address each element in your response.

SAOP Review

SAOP Review Decision:	Approved	**SAOP Review Date:**	5/29/2026
SAOP Review Comments:		**# of Days - SAOP Review:**	11

SAOP Signature

Date	User	Type	Name	Original Value	New Value
5/29/2026 2:47 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
PIA 33	Data Feed Service, pta_pia_HSRSA_Release	3/17/2026	HRSA GME program participation is on a voluntary basis	
PIA 33	Data Feed Service, pta_pia_HSRSA_Release	3/17/2026	HRSA GME program participation is on a voluntary basis	
PIA 33	Data Feed Service, pta_pia_HSRSA_Release	3/17/2026	HRSA GME program participation is on a voluntary basis	
PIA 33	Data Feed Service, pta_pia_HSRSA_Release	3/17/2026	HRSA GME program participation is on a voluntary basis	
PIA 33	Data Feed Service, pta_pia_HSRSA_Release	3/17/2026	HRSA GME program participation is on a voluntary basis	
PIA 33	Data Feed Service, pta_pia_HSRSA_Release	3/17/2026	HRSA GME program participation is on a voluntary basis	
PIA 33	PETERS, GODISGREAT	3/17/2026	HRSA GME program participation is on a voluntary basis	
PIA 33	PETERS, GODISGREAT	3/17/2026	HRSA GME program participation is on a voluntary basis	
PIA 33	PETERS, GODISGREAT	3/17/2026	HRSA GME program participation is on a voluntary basis	
PIA 33	PETERS, GODISGREAT	3/17/2026	HRSA GME program participation is on a voluntary basis	
PIA 33	PETERS, GODISGREAT	3/17/2026	HRSA GME program participation is on a voluntary basis	
PIA 33	PETERS, GODISGREAT	3/17/2026	HRSA GME program participation is on a voluntary basis	
PIA 33	PETERS, GODISGREAT	3/17/2026	HRSA GME program participation is on a voluntary basis	
PIA 33	BLAND, CRYSTAL	3/17/2026	HRSA GME program participation is on a voluntary basis	
PIA 33	BLAND, CRYSTAL	3/17/2026	HRSA GME program participation is on a voluntary basis	