US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

11/17/2017

OPDIV:

IHS

Name:

Credentialing Software

PIA Unique Identifier:

P-2870698-730027

The subject of this PIA is which of the following?

Minor Application (stand-alone)

Identify the Enterprise Performance Lifecycle Phase of the system.

Implementation

Is this a FISMA-Reportable system?

No

Does the system include a Website or online application available to and for the use of the general public?

No

Identify the operator.

Agency

Is this a new or existing system?

New

Does the system have Security Authorization (SA)?

No

Indicate the following reason(s) for updating this PIA.

Describe the purpose of the system.

The MD-Staff application is a Commercial off the Shelf (COTS) software solution to automate and standardize the data collection, storage, access and approval (decision making) credentialing process for Indian Health Service. Credentialing consists of the validation of licenser, training, education, proficiency and currency of professional healthcare skills. The purpose also includes verifying and auditing reporting systems on compliance with state, federal, and other applicable regulations.

Describe the type of information the system will collect, maintain (store), or share.

The MD-Staff application is internally hosted only within IHS servers and is intended to collect, maintain and store the following information from IHS Providers:
Provider's name, address, social security number, other identifying personal information. Provider resumes, education, certifications, experience and state issued supporting documentation. This information is then verified through several external credentialing sources (national boards, state certification agencies) to include interfaces with National Practitioner Data Bank (NPDB) Querying and Reporting Extensible Markup Language (XML) Service, System for Award Monitoring (SAM), State Licensing Boards, Drug Enforcement Agency (DEA) registration, Professional diploma, and verification of post-graduate training (specialty, residency, etc). Required information is tracked and verified in compliance with Centers for Medicare & Medicaid Services, National Committee for Quality Assurance (NCQA), Utilization Review Accreditation Commission (URAC) and The Joint Commission (TJC) requirements.

The MD-Staff system is accessed by IHS approved Providers (users) only after access is provided by internal IHS Federal Credentialing Specialists after the provider is processed through Human Resources in compliance with all Federal policies.

Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.

MD-Staff is a comprehensive, internally implemented web-based Provider credentialing system utilized to automate the credentialing data collection, management and compliance reporting process for IHS Providers. It is intended to collect, maintain and store the following information from IHS Providers:

Provider's name, address, social security number, other identifying personal information. Provider resumes, education, certifications, experience and state issued supporting documentation.

This information is then verified through several external credentialing sources (national boards, state certification agencies) to include interfaces with National Practitioner Data Bank (NPDB) Querying and Reporting Extensible Markup Language (XML) Service, System for Award Monitoring (SAM), State Licensing Boards, Drug Enforcement Agency (DEA) registration, Professional diploma, and verification of post-graduate training (specialty, residency, etc). Required information is tracked and verified in compliance with Centers for Medicare & Medicaid Services, National Committee for Quality Assurance (NCQA), Utilization Review Accreditation Commission (URAC) and The Joint Commission (TJC) requirements. This information is intended to be stored permanently according to IHS Records Management Policies for retention.

Each required type of information is utilized to verify certification from external credentialing sources noted above. The MD-Staff system does not collect information on its users to control access, since access is granted by the IHS Information Technology Access Control (ITAC) system in charge of collecting user credentials in order to grant system access.

Does the system collect, maintain, use or share PII?

Yes

Indicate the type of PII that the system will collect or maintain.

Social Security Number

Date of Birth

Name

Photographic Identifiers

Driver's License Number

Biometric Identifiers

Mother's Maiden Name

Vehicle Identifiers

E-Mail Address

Mailing Address

Phone Numbers

Medical Records Number

Medical Notes

Financial Accounts Info

Certificates

Legal Documents

Education Records

Device Identifiers

Military Status

Employment Status

Foreign Activities

Passport Number

Taxpayer ID

Letters of Reference

Professional license

Fitness Attestation

Indicate the categories of individuals about whom PII is collected, maintained or shared.

Employees

Public Citizens

Business Partner/Contacts (Federal/state/local agencies)

Vendor/Suppliers/Contractors

How many individuals' PII is in the system?

50,000-99,999

For what primary purpose is the PII used?

For identification and verification of a Medical Provider's Credentials in accordance with Centers for Medicare & Medicaid Services Conditions of Participation and third party accreditation standards.

Describe the secondary uses for which the PII will be used.

Potential secondary use of the data in the system may be to run aggregate data reports to monitor quality and run workload related reports that will not contain PII data. Additionally, auditing to ensure compliance with Medical Staff Bylaws. Professional or licensing board verifications or audits.

Describe the function of the SSN.

The Provider Social Security Number may be needed to determine if the credentialing information they provide from the University they attended is correct.

Cite the legal authority to use the SSN.

Indian Self Determination and Education and Assistance Act (25 U.S.C. 450), Snyder Act (25 U.S.C. 13), Indian Health Care Improvement Act (25 U.S.C. 1601 et seq.), Indian Health Service Transfer Act (42 U.S.C. 2001–2004).

Identify legal authorities governing information use and disclosure specific to the system and program.

Federal Information Security Management Act (FISMA), National Institute of Standards and Technology (NIST), and Health Insurance Portability and Accountability Act (HIPAA) require Indian Health Service to track federal information system users as well as their training compliance. Privacy Act of 1974 governs use and disclosure specific to use of the system.

Are records on the system retrieved by one or more PII data elements?

Yes

Identify the number and title of the Privacy Act System of Records Notice (SORN) that is being use to cover the system or identify if a SORN is being developed.

IHS Medical Staff Credentialing and Privileges Records (#09-17-0003)

September 9, 2009

October 2, 2009

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Hardcopy

Email

Online

Government Sources

Within OpDiv

Other HHS OpDiv

State/Local/Tribal

Foreign

Non-Governmental Sources

Public

Commercial Data Broker

Media/Internet

Private Sector

Identify the OMB information collection approval number and expiration date

OMB Expiration Date: 02/29/2020
OMB Approval No. 0917–0009

Is the PII shared with other organizations?

Yes

Identify with whom the PII is shared or disclosed and for what purpose.

Within HHS

CMS surveys, audits

State or Local Agencies

licensing boards

Private Sector

Credentialing files may be requested by accreditation bodies (The Joint Commission, AAAHC, etc.). Disclosures may be shared with the employee.

Describe any agreements in place that authorizes the information sharing or disclosure.

None

Describe the procedures for accounting for disclosures.

The IHS, with respect to each system of records under its direct control (i.e., Privacy Act System of Record 09-17- 0001, Medical, Health, and Billing Records) must keep a record of the date, nature, and purpose of each disclosure of a record to any person or Agency under subsection (b) of the Privacy Act (5 U.S.C. § 552a) and the name and address of the person or Agency to whom the disclosure is made. This record must be kept for 5 years or the life of the record; whichever is longer, after the disclosure for which the accounting has been made. An individual (beneficiary) is entitled, upon request, to get access to this disclosure record of his or her own personal records with the exception for disclosures made under subsection (b)(7) of the Privacy Act (as a result of civil or criminal law enforcement activity). The IHS must inform any person or other Agency about any correction or notation of dispute made by the IHS in accordance with subsection (d)(4) of the Privacy Act (Access of Records) of any record that has been disclosed to the person or Agency if an accounting of the disclosure was made. This is a mandatory reporting requirement and may be recorded utilizing the IHS- 505, "Disclosure Accounting Record" form.

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 system will have a standard Privacy Act Notice.

Is the submission of PII by individuals voluntary or mandatory?

Voluntary

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.

The collection of the Personally Identifiable Information is required and mandatory for complying with the credentialing process. There is no opt-out option. The option to opt out would be to not apply to work at Indian Health Service.

Process to notify and obtain consent from individuals whose PII is in the system when major changes occur to the system.

During the employment process the user is provided with the IHS Privacy Act Statement which includes the collection of Personal Identifiable Information is necessary for the identity proofing requirements for employment. The users consent to these terms and conditions is documented into their employee records. If a user chooses not to consent to the terms and conditions they will not be able to access the MD-Staff Application or be provided access. The individual would need to complete an IHS 810 Form.

https://intranet.hhs.gov/forms/ihs_forms.html

The Federal Warning Banner will be displayed during login that will describe that the system is a government operated system and that users can opt out of usage of the MD-Staff application at any time.

This process is repeated with each annual credentialing review. Employees can choose to continue through the re-credentialing or discontinue. Any major changes are addressed at each re-credentialing process. This is the opportunity to consent. Using the same methods as described above.

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.

Any concerns regarding the handling or management of PII within the MD-Staff application can be submitted to the IHS IT Service Desk for assignment according to the IHS Computer Security Incident Response Team Policies. An investigation will be initiated and reporting provided to the data owner. Any other actions required will be based on the nature of the incident. All complaints are addressed to the Service Unit Chief Executive Officer or (his or her) designee for investigation. Complaints are documented, maintained, and filed, and include a brief explanation of resolution, if any. Note: Complaints may also be filed directly with the Secretary, DHHS for breaches of PHI.

Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy.

Indian Health Service Privacy Official (s) will conduct periodic reviews to ensure data integrity, availability, accuracy, and relevancy, and will conduct continuous monitoring, at a minimum, monthly reviews.

Identify who will have access to the PII in the system and the reason why they require access.

Users:

Employed IHS credentialing specialists/credentialists, employed IHS staff members of respective Medical Executive Committees, and employed IHS staff members of the Governing Board will access PII in the system to perform the required credentials verification and acceptance/approval of applicants to the respective Medical Staffs. Privileges to provide clinical services cannot be granted to licensed practitioners without verification of their identity and credentials/qualifications from the PII submitted by applicants to the respective Medical Staffs.

Administrators:

For data integrity.

Developers:

For data integrity and testing purposes.

Contractors:

Direct contractors will need access to the system to review, analyze data integrity.

Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.

Indian Health Service will adhere to the National Institute of Standards and Technology (NIST) 800-53 system polices which define user provisioning and support for the application management. At this time, specific user roles and permissions have not been determined.

Describe the methods in place to allow those with access to PII to only access the minimum amount of information necessary to perform their job.

Active Directory management policies will allow for delegation of system access based on existing roles and administrators will see only the profiles of personnel who are within their Area of management. Global Group Policy.

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.

Information Systems Security Association (ISSA) training, Privacy Act and Rules of Behavior training

Describe training system users receive (above and beyond general security and privacy awareness training).

Training will be provided annually to users regarding permissible disclosure. Users who do not complete training will not will have access to the system.

Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices?

Yes

Describe the process and guidelines in place with regard to the retention and destruction of PII.

All medical staff credentials files and related documents will be maintained in accordance with the IHS Records Disposition Schedule and the Privacy Act System of Records, Memorandum No. 09-17-0003, dated September 9, 2009 and October 2, 2009.

Medical staff credential files and related documents must be retained at least 10 years after an individual's resignation or termination date from medical staff or from association with IHS.

Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.

Active Directory management for access to and management of user specific Personally Identifiable Information data is dependent on delegation policies, roles and responsibilities and will prevent unauthorized access. All changes are tracked and logged to support any audit requirements. Active Directory technical controls will prevent non-network users from gaining access. Email will be encrypted through Indian Health Service secure data transfer. An independent audit will be conducted annually.

Note: web address is a hyperlink.