US Department of Health and Human Services
Indian Health Service
Privacy Impact Assessment

Date Signed:

3/2/2016

OPDIV:

IHS

Name:

IHS Resource Patient Management System (RPMS)

PIA Unique Identifier:

P-8726602-254322

The subject of this PIA is which of the following?

Major Application

Identify the Enterprise Performance Lifecycle Phase of the system.

Operations and Maintenance

Is this a FISMA-Reportable system?

Yes

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

Yes

Identify the operator.

Agency

Is this a new or existing system?

Existing

Does the system have Security Authorization (SA)?

Yes

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

New Interagency Uses

Describe the purpose of the system.

IHS Resource Patient Management System (RPMS) - The RPMS is a clinical and patient administrative information system that supports the management of the healthcare needs of the American Indian and Alaska Natives populations.

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

1. Health and medical records containing examination, diagnostic and treatment

data, proof of IHS eligibility, social data (such as name, address, date of birth, Social Security Number (SSN), tribe), laboratory test results, and dental, social service, domestic violence, sexual abuse and/or assault, mental health, and nursing information.

2. Follow-up registers of individuals with a specific health condition or a particular health status such as cancer, diabetes, communicable diseases, suspected and confirmed abuse and neglect, immunizations, suicidal behavior, or disabilities.
3. Logs of individuals provided health care by staff of specific hospital or clinic departments such as surgery, emergency, obstetric delivery, medical imaging, and laboratory.
4. Surgery and/or disease indices for individual facilities that list each relevant individual by the surgery or disease.
5. Monitoring strips and tapes such as fetal monitoring strips and EEG and EKG tapes.
6. Third-party reimbursement and billing records containing name, address, date of birth, dates of service, third party insurer claim numbers, SSN, health plan name, insurance number, employment status, and other relevant claim information necessary to process and validate third-party reimbursement claims.
7. Contract Health Service (CHS) records containing name, address, date of birth, dates of care, Medicare or Medicaid claim numbers, SSN, health plan name, insurance number, employment status, and other relevant claim information necessary to determine CHS eligibility and to process CHS claims.
8. Yes, contains IIF.
9. Mandatory submission of personal information.

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

- Social Security Number
- Name
- Phone Numbers
- Medical Notes
- Education Records
- Military Status
- Date of Birth
- Mailing Address

- Medical Records Number
- Financial Account Info
- Legal Documents,
- Employment Status
- Chart No.,
- TIN
- DUNS
- Provider License #

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

- Employees
- Public Citizens
- Business Partners/Contacts (Federal, state, local agencies)
- Vendors/Suppliers/Contractors
- Patients

For what primary purpose is the PII used?

1. Records may be disclosed to Federal and non-Federal (public or private) health care providers that provide health care services to IHS individuals for purposes of planning for or providing such services, or reporting results of medical examination and treatment.
2. Records may be disclosed to Federal, state, local or other authorized organizations that provide third-party reimbursement or fiscal intermediary functions for the purposes of billing or collecting third-party reimbursements. Relevant records may be disclosed to debt collection agencies under a business associate agreement arrangement directly or through a third party.
3. Records may be disclosed to state agencies or other entities acting pursuant to a contract with CMS, for fraud and abuse control efforts, to the extent required by law or under an agreement between IHS and respective state Medicaid agency or other entities.
4. Records may be disclosed to school health care programs that serve AI/AN for the purpose of student health maintenance.
5. Records may be disclosed to the Bureau of Indian Affairs (BIA) or its contractors under an agreement between IHS and the BIA relating to disabled

AI/AN children for the purposes of carrying out its functions under the Individuals with Disabilities Education Act (IDEAS), 20 U.S.C. 1400, et seq.

6. Records may be disclosed to organizations deemed qualified by the Secretary of DHHS and under a business associate agreement to carry out quality assessment/improvement, medical audits, utilization review or to provide accreditation or certification of health care facilities or programs.
7. Records may be disclosed under a business associate agreement to individuals or authorized organizations sponsored by IHS, such as the National Indian Women's Resource Center, to conduct analytical and evaluation

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

Yes

Is the PII shared with other organizations?

Yes

A. New patients must be registered in the IHS facility data base prior to being provided health care services; however, emergency services should not be delayed. Information on patients who present a critical emergency that requires immediate medical attention must be obtained from the patient's relative or other accompanying individual. Each patient's IHS registration information is updated on each subsequent visit to the facility by personal interview conducted by a designated IHS facility staff member. The patient registration process at each IHS facility is accomplished by using the IHS Patient Registration System (PRS) software and the technical guidelines in Chapter 2, "Patient Registration" of the IHS Business Office Manual.
B. The service unit has the responsibility to encourage all patients who are registered to present any documentation they might have relative to their eligibility-for IHS health care services and alternate resources. These documents will greatly assist in maintaining accurate patient information in the PRS data base.
C. Patients are requested to bring their Social Security card, private insurance identification, and other information (such as proof of tribal affiliation and blood quantum) to initial or subsequent patient registration interviews. Registration staff explains to the patients that such information will expedite the patient registration and eligibility determination process. Patients' mailing addresses and personal information files are kept updated so that all health care

benefits can be identified and expedited, and be utilized by the health care provider.

D. All IHS staff are sensitive to IHS patient's cultural values and concerns for privacy. Patient registration is a vital part of each IHS facility's public relations program and patient registration staff receive continuous management support for maintaining skills in communicating with the patients and assuring the patients' comfort during the interview process.
E. Confidentiality of patient information collected is maintained at all times in accordance with the Privacy Act of 1974. The registration staff periodically reviews the Privacy Act. The registration staff informs the patient of the requirements of the Privacy Act, and the date is entered into the PRS.
F. The patient must authorize release of Medicare/Railroad Insurance information, and the date the authorization was obtained is entered into the PRS by registration staff.

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

Provided locally at patient check in process in accordance with Privacy and HIPAA regulations

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.

A. Changes to local systems are transported to the NPIRS for processing.
B. Individual service units are responsible for addressing concerns, and the patient may escalate to higher authority, e.g., the IHS Privacy Act Officer. Patients may file complaints directly to the Secretary, HHS through the OCR HIPAA website (under the authority of the HIPAA Privacy Rule)

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

Yes

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

- Users: Access is limited to authorized IHS personnel and IHS contractors and subcontractors in the performance of their duties.

    - Authorized personnel include: Medical records personnel, health care providers, authorized researchers, medical audit personnel, and health care team members, and, administrative personnel on a need to know basis.
- Administrators: Access is limited to authorized IHS personnel and IHS contractors and subcontractors in the performance of their duties.
    - Authorized personnel include: Medical records personnel, health care providers, authorized researchers, medical audit personnel, and health care team members, and, administrative personnel on a need to know basis.
- Developers: Access is limited to authorized IHS personnel and IHS contractors and subcontractors in the performance of their duties.
    - Authorized personnel include: Medical records personnel, health care providers, authorized researchers, medical audit personnel, and health care team members, and, administrative personnel on a need to know basis.
- Contractors: Access is limited to authorized IHS personnel and IHS contractors and subcontractors in the performance of their duties.
    - Authorized personnel include: Medical records personnel, health care providers, authorized researchers, medical audit personnel, and health care team members, and, administrative personnel on a need to know basis.

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. Patient listings which may identify individuals are maintained in IHS Area and Program Offices permanently. Inactive records are held at the facility which provided health services from three to seven years and then are transferred to the appropriate Federal Records Center. Monitoring strips and tapes (i.e., fetal monitoring strips and EEG and EKG tapes) which are not stored in the patient's official medical record, are stored at the health facility for one year and are then transferred to the appropriate Federal Records Center. (See Appendix 2 for Federal Record Center addresses). Records, including those maintained on computer media are retained in useable formats at the Regional Federal Records Centers for 25 years. Disposal methods include burning or shredding of hard copy and erasing of magnetic media.

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

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage: File folders, ledgers, card files, microfiche, microfilm, computer tapes, disk packs, digital photo discs, and automated, computer-based or electronic files.

Retrievability: Indexed by name, record number, and SSN and cross-indexed.

Safeguards: Safeguards apply to records stored on-site and off-site.

1. Authorized Users: Access is limited to authorized IHS personnel, volunteers, IHS contractors, subcontractors, and other business associates in the performance of their duties. Examples of authorized personnel include: Medical records personnel, business office personnel, contract health staff, health care providers, authorized researchers, medical audit personnel, health care team members, and legal and administrative personnel on a need to know basis.
2. Physical Safeguards: Records are kept in locked metal filing cabinets or in a secured room or in other monitored areas accessible to authorized users at all times when not actually in use during working hours and at all times during non-working hours. Magnetic tapes, disks, other computer equipment (e.g., pc workstations) and other forms of personal data are stored in areas where fire and life safety codes are strictly enforced. Telecommunication equipment (e.g., computer terminal, servers, modems and disks) of the Resource and Patient Management System (RPMS) are maintained in locked rooms during non-working hours. Network (Internet or Intranet) access of authorized individual(s) to various automated and/or electronic programs or computers (e.g., desktop, laptop, handheld or other computer types) containing protected personal identifiers or personal health information (PHI) is reviewed periodically and controlled for authorizations, accessibility levels, expirations or denials, including passwords, encryptions or other devices to gain access. Combinations and/or electronic pass cards on door locks are changed periodically and whenever an IHS employee resigns, retires or is reassigned.
3. Procedural Safeguards: Within each facility a list of personnel or categories of personnel having a demonstrable need for the records in the performance of their duties has been developed and is maintained. Procedures have been developed and implemented to review one-time requests for disclosure to personnel who may not

be on the authorized user list. Proper charge-out procedures are followed for the removal of all records from the area in which they are maintained. Records may not be removed from the facility except in certain circumstances, such as compliance with a valid court order or shipment to the Federal Records Center(s). Persons who have a need to know are entrusted with records from this system of records and are instructed to safeguard the confidentiality of these records. These individuals are to make no further disclosure of the records except as authorized by the system manager and permitted by the Privacy Act and the HIPAA Privacy Rule as adopted, and to destroy all copies or to return such records when the need to know has expired. Procedural instructions include the statutory penalties for noncompliance. The following automated information systems (AIS) security procedural safeguards are in place for automated health and medical records maintained in the RPMS. A profile of automated systems security is maintained. Security clearance procedures for screening individuals, both Government and contractor personnel, prior to their participation in the design, operation, use or maintenance of IHS AIS are implemented. The use of current passwords and log-on codes are required to protect sensitive automated data from unauthorized access. Such passwords and codes are changed periodically. An automated or electronic audit trail is maintained and reviewed periodically. Only authorized IHS Division of Information

Does the website have a posted privacy notice?

Yes

Does the website use web measurement and customization technology?

No

Does the website have any information or pages directed at children under the age of thirteen?

No