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

Date Signed:

3/2/2016

OPDIV:

IHS

Name:

IHS National Patient Information Reporting System

PIA Unique Identifier:

P-3904086-331244

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?

No

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. Describe the purpose of the system.

New Interagency Uses

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.

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
- Name
- Military Status
- Date of Birth
- Medical Records Number

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

shared.

- Business Partners/Contacts (Federal, state, local agencies)
- Vendors/Supplies/Contractors
- Patients

How many individuals' PII is in the system?

One million or more

For what primary purpose is the PII used?

1. Does not violate legal or policy limitations under which the record was provided, collected, or obtained.
2. Law Enforcement Agencies: The IHS health care providers may disclose information from these records regarding the commission of crimes or the occurrence of communicable diseases, tumors, suspected child abuse, births, deaths, alcohol or drug abuse, etc., as required by Federal law or regulation or State or local law or regulation of the jurisdiction in which the facility is located. The IHS health care providers may disclose information from these records regarding suspected cases of child abuse.
3. IHS Contractors: Records may be disclosed to an IHS contractor, including tribal contractors, for the purpose of computerized data entry or maintenance of records contained in this system. The contractor shall be required to maintain Privacy Act safeguards with respect to the receipt and processing of such records. Records may be disclosed to a health care provider under contract to IHS (including tribal contractors) to permit the contractor to obtain health and medical information about the subject individual in order to provide appropriate health services to that individual. The contractor shall be required to maintain Privacy Act safeguards with respect to the receipt and processing of such records.
4. Student Volunteers: Records may be disclosed to student volunteers, individuals working under a personal services contract, and other individuals performing functions for PHS who do not technically have the status of agency employees, if they need the records in the performance of their agency functions. The information is shared back to the customers in support of their regional programs. Information (i.e., statistical, patient demographic, facility or

institutional, medical, research, education, disease management, eligibility, etc.) is shared with internal IHS agencies and external organizations with approvals from IHS/OPS and HIPAA.

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

Yes

Is the PII shared with other organizations?

Yes

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.

1. Notification procedure

    a. General Procedure: Requests must be made to the appropriate System Manager (IHS Area, Program Office Director or Service Unit Director/Chief Executive Officer). A subject individual who requests a copy of, or access to, his or her medical record shall, at the time the request is made, designate in writing a responsible representative who will be willing to review the record and inform the subject individual of its contents. Such a representative may be an IHS health professional. When a subject individual is seeking to obtain information about himself/ herself that may be retrieved by a different name or identifier than his/her current name or identifier, he/she shall be required to produce evidence to verify that he/she is the person whose record he/she seeks. No verification of identity shall be required where the record is one that is required to be disclosed under the Freedom of Information Act. Where applicable, fees for copying records will be charged in accordance with the schedule set forth in 45 CFR Part 5b.

    b. Requests In Person: Identification papers with current photographs are preferred but not required. If a subject individual has no identification but is personally known to the designated agency employee, such employee shall make a written record verifying the subject individual's identity. If the subject individual has no identification papers, the responsible system manager or designated agency official shall require that the subject individual certify in writing that he/she is the individual whom he/she claims to be and that he/she understands that the knowing and willful request or acquisition of records concerning an individual under false pretenses is a

criminal offense subject to a $5,000 fine. If an individual is unable to sign his/her name when required, he/she shall make his/her mark and have the mark verified in writing by two additional persons.

c. Requests By Mail: Written requests must contain the name and address of the requester, his/her date of birth and at least one other piece of information that is also contained in the subject record, and his/her signature for comparison purposes. If the written request does not contain sufficient information, the System Manager shall inform the requester in writing that additional, specified information is required to process the request.

d. Requests by Telephone: Since positive identification of the caller cannot be established, telephone requests are not honored.

e. Parents, Legal Guardians and Personal Representatives: Parents of minor children and legal guardians or personal representatives of legally incompetent individuals shall verify their own identification in the manner described above, as well as their relationship to the individual whose record is sought. A copy of the child's birth certificate or court order establishing legal guardianship may be required if there is any doubt regarding the relationship of the individual to the patient.

2. Record access procedures

    a. Same as Notification Procedures: Requesters may write, call or visit the last IHS facility where medical care was provided. Requesters should also provide a reasonable description of the record being sought. Requesters may also request an accounting of disclosures that have been made of their record, if any.

3. Contesting record procedures: Requesters may write, call or visit the appropriate IHS

    a. Area/Program Office Director or Service Unit Director/Chief Executive Officer at his/her address specified in Appendix 1, and specify the information being contested, the corrective action sought, and the reasons for requesting the correction, along with supporting information to show how the record is inaccurate, incomplete, untimely, or irrelevant.

b. Record source categories: Individual and/or family members, IHS health care personnel, contract health care providers, State and local health care provider organizations, Medicare and Medicaid.

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

Part of patient enrollment process at the local site. 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 to resolve an individual's concerns when they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate.

File complaint at local facility in accordance with Privacy Act

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

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.

Retention of data is retained minimally to three years back for User Population reporting

in support of Congressional requirements. Additional retention of historical data is maintained to the extent possible in support of data sharing requests. Destruction requirements are detailed in Security Operating Procedure 02-20, titled Media Destruction. Disposition is in line with existing MOUs, MOAs and other agreements, if applicable.

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.