US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

05/12/2025

OPDIV:

IHS

Name:

Four Directions Hub

PIA Unique Identifier:

P-5983360-018828

The subject of this PIA is which of the following?

Major Application

Identify the Enterprise Performance Lifecycle Phase of the system.

Implementation

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)?

No

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

PIA Validation

Describe in further detail any changes to the system that have occurred since the last PIA.

No changes

Describe the purpose of the system.

The Four Directions Hub (4DH) is a central point supporting health information exchange (HIE) within the Indian health care system, as well as with external entities that provide healthcare-related services to American Indian and Alaska Native (AI/AN) people. The Indian health care system includes Indian Health Service (IHS) hospitals and clinics, health care facilities operated by self-governing Indian Tribes, and Urban Indian health care facilities; these are collectively known as the I/T/U. External entities will include a number of federal agencies as well as state, academic, and private health care partners that also serve AI/AN people (see below).

The purpose is to ensure that providers have access to information about patients' health conditions, medications, allergies, test results, etc. because this information is critical to improving quality of care and reducing both risks and costs. 4DH is recognized as a key factor in improving quality of

care by numerous government mandates including the Trusted Exchange Framework and Common Agreement (TEFCA) and Federal Health IT Certification Programs.

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

All information collected relates to health care services, including information needed to correctly and uniquely identify the patient, information about patients' health conditions and their treatment, and information relating to payment for services. Information includes demographics - name, preferred name, sex, social security number (SSN), driver license, device identifier, and employment status. physical and mailing address, email address, phone, date of birth, mother's maiden name, race and ethnicity. Also includes information from the medical record - medical record number, appointments, dates of visits and hospitalizations, diagnoses, laboratory, imaging and other test results, allergies and adverse reactions, prescriptions and medication lists, narratives such as clinic notes, operative notes, consult notes, and hospital discharge summaries, insurance eligibility information, codes used for billing purposes.

User account information is stored in the system as user names, user first/last names, and passwords.

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

The 4DH is a repository for patient health data contributed from participating I/T/U healthcare entities, submitted in the form of structured documents complying with the Consolidated Clinical Document Architecture (CCDA) and related standards. These documents include information about patient demographics, medical problems and other health issues, clinical notes such as hospital discharge summaries, allergies, medications, test results, immunizations, etc. These data are consolidated in the 4DH and made available to authorized users who are providing care for the patient and need to have information about problems, allergies, medications, and care received at other facilities, in order to provide the best possible care and reduce risks of dangerous medication interactions, overtesting/overimmunizing, failing to recognize conditions being treated elsewhere, etc. Medical providers at I/T/U facilities will be able to access this information through a secure web portal, and download structured data for incorporation into their local electronic health record (EHR) systems. The 4DH has a secure connection to the national eHealth Exchange, through which users will be able to search for and retrieve clinical information about American Indian and Alaska Native (AI/AN) patients receiving care through the Department of Veterans Affairs (VA), Department of Defense (DoD), or any of the multiple private sector entities that are connected to eHealth Exchange either directly or through their regional or state HIEs. The 4DH is not the source of record for patient data. This data all derives from EHRs and related systems at the local care facilities, and cannot be added to, deleted or modified by any users of the 4DH - only viewed and downloaded. The 4DH is not a permanent data repository; data will be retained in accordance with regulations governing comparable HIE repositories. Current plans are to retain data for seven (7) years after last accessed.

Users of the system include clinicians, medical records administrators tasked with validating patient matches and consent elections, and system administrators. Information collected on these is limited to full name, user ID, affiliation and location (e.g., Indian Health Service, Rockville MD). Authentication processes are handled by separate Identity and Access Management systems so no passwords are stored in 4DH.

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

Driver's License Number
Mother's Maiden Name
E-Mail Address
Mailing Address
Phone Numbers
Medical Records Number
Medical Notes
Device Identifiers
Employment Status
User Credentials
Sex
race and ethnicity

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

Employees
Public Citizens
Patients
User Credentials for administrators

How many individuals' PII is in the system?

1,000,000 or more

For what primary purpose is the PII used?

PII is used for coordination of health care services among providers, to improve care and outcomes, and reduce risk to patients.

Users of the system include clinicians, medical records administrators tasked with validating patient matches and consent elections, and system administrators. System administrative accounts are used for auditing of system usage and validation of functionality. Information collected on these is limited to full name, user ID, affiliation and location (e.g., Indian Health Service, Rockville MD). Authentication processes are handled by separate Identity and Access Management systems so no passwords are stored in 4DH.

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

Secondary use of patient data provided to authorized external users through the TEFCA network will be governed by the standard TEFCA agreement. Data in the 4DH may be used to supplement other data being submitted to the IHS National Patient Information Reporting System (NPIRS) for the purposes of agency reporting on quality and performance measures - such as the GPRA Modernization Act (GPRAMA) - to Department of Health and Human Services (HHS) and the Office of Management and Budget (OMB), and other agency-level business analytics. However, no PII will be used for these purposes, only non-identifiable demographic and clinical information. Secondary use of patient data provided to authorized external users through the eHealth Exchange will be governed by the standard Data Use and Reciprocal Support Agreement (DURSA) with which all participants on the eHealth Exchange must agree to comply.

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

Departmental Regulations (5 U.S.C.
301); Privacy Act of 1974 (5 U.S.C. 552a); Federal Records Act (44 U.S.C. 2901); Section 321 of the Public Health Service Act, as amended (42 U.S.C. 248); Section 327A of the Public Health Service Act, as amended (42 U.S.C. 254a); Snyder Act (25 U.S.C. 13); Indian Health Care

Improvement Act (25 U.S.C. 1601 et seq.); Transfer Act of 1954 (42 U.S.C. 2001–2004); HIPAA, Privacy Act, HITECH (and subsequent regulations); and 21st Century Cures Act, 42 CFR Part 2.

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 System No. 09-17-0005, “Personal Health Records (PHR) Administrative Records—IHS”.

IHS System No. 09-17-0001, “Medical, Health and Billing Records.”

Identify the sources of PII in the system.

Government Sources

Within OpDiv

State/Local/Tribal

Other Federal Entities

Non-Government Sources

Public

Private Sector

Identify the OMB information collection approval number and expiration date

PRA does not apply.

Is the PII shared with other organizations?

Yes

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

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

The connection to the TEFCA network is governed by TEFCA, a standard document that must be signed and adhered to by all participants. Tribal and Urban Indian healthcare organizations connecting directly to the 4DH will sign a Multi-Purpose Agreement with IHS that incorporates elements of TEFCA as well as the HIPAA-required Business Associate Agreement (BAA), the IHS-required Interconnection Security Agreement (ISA), Memorandum of Understaning (MOU) and the End User Agreement for Direct secure messaging.

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.

All transmissions of patient information from the Four Directions Hub occur electronically, either to entities that have completed binding agreements and rigorous technical testing, or to clinician users who are employed by those entities, appropriately credentialed and authenticated to access this information. The 4DH system logs all connections, queries, and responses to those queries, and retains these logs in accordance with applicable law.

Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason.

Indian Health Manual - Part 2, Chapter 7 - It is IHS policy to provide adequate notice of its uses and disclosures of PHI and of the individual's rights and IHS' legal duties with respect to PHI. A copy of the Notice is provided to new patients, patients whose charts are reactivated, and patients who reach legal age. The Patient Registration Office provides a copy of the current Notice to the patient. The staff member has the patient acknowledge receipt of the Notice by signing the Acknowledgment of Receipt of IHS Notice of Privacy Practices. The signed "Acknowledgement of Receipt of IHS Notice of Privacy Practices" is filed into the patient's medical record.

All non-IHS entities (self-governance tribes and urban Indian healthcare organizations) that connect to the IHS 4DH are obligated under HIPAA to provide notices of privacy practices to their patients. They are further obligated under the Multi-Purpose Agreement that governs their connections to the 4DH to confirm their commitment to and compliance with applicable laws and regulations concerning such notices.

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 initial collection of PII occurs at the various healthcare facilities, and permission to collect this information is out of scope of the Four Directions Hub. All federal (IHS) sites have patient data exported to the 4DH as encounters occur or are updated, because the 4DH is an extension of the IHS system of medical records. Any Tribal/Urban facility agreeing to participate in the 4DH will similarly send all patient encounter data. This creates a more complete record for all patients whose data is contributed by participating I/T/U facilities. Any authorized user from a participating organization may search for and view data in the 4DH in order to improve care services. As currently designed, there is no separate consent process for sharing patient data within the I/T/U ecosystem.

Patient consent elections are applied at the gateway to TEFCA. All patients at all facilities are provided with a Notice of Privacy Practices. They are also offered Form IHS-810, "Authorization for Use or Disclosure of Protected Health Information". By completing and signing this document, patients may consent to or decline sharing of their protected health information with external entities outside the I/T/U ecosystem through the Exchange.

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

It is IHS policy to provide adequate notice of its uses and disclosures of PHI/PII and of the individual's rights and IHS' legal duties with respect to PHI/PII. The IHS prominently and clearly displays the Notice (2-7.18) in every facility (http://www.hipaa.ihs.gov/). A copy of the Notice is also provided to new patients, patients whose charts are reactivated, and patients who reach legal age. The Patient Registration Office or other appropriate department provides a copy of the current Notice to the patient. The patient acknowledges receipt of the Notice by signing the Acknowledgment of Receipt of IHS Notice of Privacy Practices. An IHS staff member signs and dates the

Acknowledgement form and files the signed "Acknowledgement of Receipt of IHS Notice of Privacy Practices" into the patient's medical record. No less than every three years, IHS provides notification of the availability of the Notice and how to obtain the Notice.

If a patient, upon reviewing the terms of the Notice of Privacy Practices, elects to change their consent for Health Information Exchange, they indicate so on the appropriate IHS official form, assisted by staff at the healthcare facility. This consent election is securely transmitted to the 4DH system and the exchange settings for that patient are updated as requested.

If the 4DH system undergoes a material change impacting the way PII is collected or used, a revised Notice of Privacy Practices must be posted in clear and prominent locations in every facility and on its web site, on or after the effective date of the revision. The revised Notice will be posted on the IHS website within 60 days of a material revision. The revised Notice is also given to all patients who come into a facility after the effective date of the revision and is available upon request on or after the effective date of the revision. Additionally, IHS provides the revised notice to all eligible patients registered in the patient registration system within 60 days of the revision of the Notice. Any individual, whether or not a patient, has the right to request and receive a copy of the Notice at any time, except an inmate. Inmates have no rights to the Notice (45 CFR § 164.520 (a)(3)).

The IHS will notify all non-IHS entities (self-governance tribes and urban Indian healthcare organizations) that connect to the IHS 4DH of any major changes to the 4DH that would warrant updating of notices of privacy practices that they share with their patients. These entities are obligated under the terms of the Multi-Purpose Agreement that governs their connections to the 4DH to confirm their commitment to and compliance with applicable laws and regulations concerning such notices.

User and administrative accounts are managed via the IHS ServiceNow system. This system used is to enable qualified IHS personnel to submit requests for access to computer and network resources. Appropriate supervisors can submit new access, update access or remove access requests for their team members, as well as perform required annual access reviews and team management functions.

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 a patient concern relates to accuracy of information stored in or shared by the 4DH, they are referred back to the healthcare entity that submitted the information in question to 4DH, as the 4DH is not the definitive source record and has no power to change the information. If the concern is about inappropriate sharing or transmission of patient information from 4DH, this will be investigated in detail by the system administrators at the IHS Office of Information Technology to ascertain the nature of the disclosure, the authentication of the querying person or entity, and any other relevant information.

Within IHS, all complaints are addressed to the Service Unit Chief Executive Officer or designee for investigation. Complaints are documented, maintained, and filed, and include a brief explanation of resolution, if any. Tribal and Urban Indian healthcare organizations are required under HIPAA and the terms of the Multi-Purpose Agreement to have comparable processes at their facilities. Note: Complaints may also be filed directly with the Secretary, DHHS.

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

Integrity: The 4DH receives data from contributing IHS, Tribal, and Urban Indian Organizations via connections that have automated processes, such as data encryption and hashing, to ensure that data received has not been corrupted in transit and accurately reflects the data sent by the contributing site. Data that does not conform to published content and structure standards, including

the Admit, Discharge, Transfer (ADT) and Consolidated Clinical Document Architecture (CCDA) standard, is not accepted. These processes are continuously monitored, as thousands of documents are received and processed from contributing sites on a daily basis.

Availability: The 4DH has automated processes in place for backup and disaster recovery to ensure high levels of availability. The cloud service provider for 4DH - Microsoft Azure - ensures continuous availability well above 99%.

Accuracy and Relevancy: All of the PII and other data accepted into the 4DH is derived from authoritative sources such as local EHRs and is accepted from these systems as accurate and relevant.

Per IHS policy, ServiceNow supervisors are required to annually audit their staff and systems access and authorization level. If a user's role has changed, their access is updated or revoked and systems accesses are disabled.

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

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

Indian Health Manual, Part 8, Chapter 21 - Access Control.
IHS system administrators and users are granted role-based access following ServiceNow processes wherein supervisors request and justify specific access privileges for appropriate employees. Non-IHS entities connected to 4DH are obligated under the terms of the Multi-Purpose Agreement which governs those connections to enforce comparable requirements for their employees. No non-IHS individuals are granted administrative access to the system.

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.

The system utilizes least privilege and role-based access controls. All administrators of the Four Directions Hub are IHS employees or contractors who have undergone rigorous background clearance. All other users of the system are credentialed medical professionals either at IHS facilities or participating tribal or urban Indian healthcare organizations. These users are required, by training and the ethical standards of their profession, enforced by state licensing, specialty boards, and facility credentialing practices, to access any medical record system including the 4DH only on a need-to-know basis for patients under their care.

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.

Role-based training, IHS Rules of Behavior agreements, and Information System Security and Privacy Awareness training courses are required to be completed annually by all IHS users. Non-IHS entities with connections to the 4DH are obligated under the terms of the Multi-Purpose Agreement to provide comparable training to their users of the system. All administrators of the 4DH are IHS employees or contractors.

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

Initial training will be conducted by IHS Office of Information Technology staff and contractors for users and technical support staff at initial test and pilot sites. These will be a combination of interactive virtual training and live sessions. A "train the trainer" element will be included, such that regional (IHS Area) trainers will assume responsibility for training users at sites in their Areas as they on-board to the 4DH. Training and support materials available to users on a perpetual basis include quick reference job aides, full user manuals, and recorded webinars.

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.

General Records Schedule 5.2: Transitory and Intermediary Records. TEMPORARY. Destroy when no longer needed for
business use, or according to agency predetermined time period or business rule.

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

The IHS 4DH is hosted in the Azure Government Cloud, certified FedRAMP HIGH, which is the highest level of security for cloud-hosted systems. Government Cloud systems are both logically and physically separated from all non-government systems, and the Cloud Service Provider ensures robust data security, high availability, and disaster recovery. All transmissions into and from the 4DH are encrypted (SHA-256). Administrators of Infrastructure as a Service (IaaS) hosted in the Government Cloud must be U.S. citizens that have cleared rigorous background investigations.

4DH System Security Plan documents administrative, technical and physical controls that are inherited from Azure Cloud Provider, IHS Enterprise IT and 4DH System Implemented controls. The following examples provide control families from NIST 800-53 and part of 4DH SSP.

Technical Controls Examples–

- Access Controls – AC-1 to AC-25
- Audit and Accountability – AU-1 to AU-16
- Identification and Authentication – IA-1 to IA-11

Administrative Controls Examples –

- Planning – PL-1 to PL-9
- Risk Assessment – RA-1 to RA-6
- System and Services Acquisition – SA-1 to SA-22

Physical Controls Examples –

- Physical and Environmental Protection – PE-1 to PE-20
- Systems and Communications Protection – SC-1 to SC44