US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

06/02/2026

OPDIV:

IHS

Name:

Instrument-based vision screeners

PIA Unique Identifier:

P-5802349-108752

The subject of this PIA is which of the following?

General Support System (GSS)

Identify the Enterprise Performance Lifecycle Phase of the system.

Operations and Maintenance

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 Spot Vision Screener is a handheld medical device used by IHS healthcare staff to quickly check a patient's vision, especially in young children who may not be able to complete a traditional eye chart test. It supports IHS clinical care and preventive screening functions by identifying potential vision problems, such as nearsightedness or eye alignment issues, in a matter of seconds. For these functions, the system captures an image of the patient's eyes from a short distance, analyzes the results automatically, and provides a simple report to the healthcare provider to help determine whether the patient may need further evaluation or referral for eye care.

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

The Spot Vision Screener collects and uses limited Personally Identifiable Information (PII) about patients and minimal PII regarding staff. For patients, the system captures an image of the eyes and generates vision screening results, which may be associated with basic identifying information such as the patient's name, date of birth, medical record number, medical notes, photographic identifiers, and the date and time of the screening. Because these results relate to an individual's health, they

are considered protected health information (PHI). For staff, the system may record limited information such as a user ID or operator name to show who performed the screening, which is considered personally identifiable information (PII). The system may store this information temporarily on the device or transmit it to an electronic health record system. Records are typically retrieved using patient identifiers such as name, date of birth, or medical record number, rather than by staff information.

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

The Spot Vision Screener is a handheld medical device used by healthcare staff to quickly check a patient's vision, especially in children, by taking a picture of the eyes and automatically analyzing it for potential vision concerns. The system collects and temporarily stores information about patients, including images of the eyes, photographic identifiers, medical notes, vision screening results, and basic identifying details such as name, date of birth, medical record number, and the date and time of the screening. This information is considered protected health information (PHI) because it relates to an individual's health. The device may also collect limited staff information, such as a user ID or operator name, to record who performed the screening, which is considered personally identifiable information (PII). In addition to PHI/PII, the system may collect general technical information, such as device ID, screening settings, and timestamps, to support operation and recordkeeping. Information may be stored on the device for a short period and/or transmitted to an electronic health record system where it becomes part of the patient's medical record. Records are routinely retrieved using patient identifiers such as name, date of birth, or medical record number; staff information is not typically used to retrieve records.

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

Yes

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

Date of Birth
Name
Photographic Identifiers
Medical Records Number
Medical Notes
date and time of the screening
employee user ID
operator name preforming the screening

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

Employees
Patients

How many individuals' PII is in the system?

100,000-999,999

For what primary purpose is the PII used?

The primary purpose of the PII collected by the system is to accurately identify the patient and ensure that the correct vision screening results are associated with the correct individual's medical record. This supports safe and effective patient care by allowing healthcare providers to review results, make appropriate clinical decisions, and, if needed, refer the patient for further evaluation. Limited staff PII is used to document which employee performed the screening for accountability and recordkeeping purposes.

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

Secondary uses of the PII/PHI collected by the system are limited and support healthcare operations rather than direct patient care. These may include quality assurance and performance improvement activities, such as reviewing screening accuracy and outcomes; administrative and recordkeeping functions, including documentation and audit trails; training purposes to ensure staff are properly using the device; and reporting or compliance activities, such as accreditation reviews or internal oversight. In all cases, the information is used in accordance with applicable privacy and security requirements and is not the primary purpose for which it was collected.

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

5 U.S.C. 301, Departmental Regulations; 5 U.S.C. 552a, Privacy Act of 1974; 4 U.S.C. 2901, Federal Records Act; 42 U.S.C. 248, Section 321 of the Public Health Service Act, as amended; 42 U.S.C. 254a, Section 327A of the Public Health Service Act, as amended; 25 U.S.C. 13, Snyder Act; 25 U.S.C. 1601 et seq., Indian Health Care Improvement Act; and 2 U.S.C. 2001-2004, Transfer Act of 1954.

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.

09-17-0001, Medical, Health, and Billing Records Systems

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 OpDiv

State

Foreign

Other Federal Entities

Non-Government Sources

Public

Commercial Data Broker

Media/Internet

Private Sector

Identify the OMB information collection approval number and expiration date

Exempt from OMB Information Collection Number through Public Law 114-255, the 21st Century Cures Act, Section 2035: Exemption for IHS from the Paperwork Reduction Act requirements.

Is the PII shared with other organizations?

No

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 Protected Health Information (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. A copy of the notice is given to the patient upon establishing a record or when requested. The staff member providing the notice has the patient acknowledge receipt of the Notice by signing the Acknowledgment of Receipt of IHS Notice of Privacy Practices. The signed Acknowledgment of Receipt of IHS Notice of Privacy Practices" is filed into the patient's medical record. The notices are displayed in the facility as well as on IHS website. IHS employees are notified at the time of hire that their Personally Identifiable Information (PII) will be collected and give consent as it is part of the on-boarding process.

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.

Per the policy provided in the Indian Health Manual Part 2 Chapter 7 Section 22, "Under the Under the Health Insurance Accountability and Potability Act Privacy Rule, patients have the right to request restriction(s) of the use and/or disclosure of their PHI to carry out treatment; payment and health care operations; inpatient hospital directory; and disclosures to relatives, family members, personal representatives, close friends, health care givers, and any other person involved in the patient's care or payment who is identified by the patient. The IHS is not required to agree to the request. However, a patient still may object to the disclosure of information for the inpatient hospital directory and to relatives, friends, and others involved in patient care under 45 CFR 164.510(b). See Section 2-7.19, "Procedure for the Uses and Disclosures of Protected Health Information for Involvement in the Patient's Care and for Notification Purposes."

The initial collection of PII occurs at the various healthcare facilities at the point of registration and is required to determine eligibility for services. 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 4DH and eHealth 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 in every facility. 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 the Notice is revised by a material change, the revised Notice 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 the 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)).

IHS employees are notified at the time of hire that their PII will be collected and give consent as it is part of the on-boarding process.

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.

According to IHS policy all complaints regarding HIPAA Privacy and Privacy Act violations shall be addressed to the Chief Executive Officer or designee. Complaints must be documented, maintained, and filed, and include a brief explanation of resolution, if any. Note: Individuals may also file complaints directly to the Secretary, Department of Health and Human Services (HHS).

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

Healthcare staff and privacy/security personnel periodically review the data stored on the device and in the electronic health record system to confirm that records are complete and correctly associated with the right patient. This review may include checking that patient identifiers (name, date of birth, medical record number) are accurate, ensuring that staff user IDs are properly recorded, and verifying that any temporarily stored data on the device has been securely transmitted or deleted. Routine audits and scheduled data reviews help maintain data integrity, compliance with privacy regulations, and the secure handling of PHI and PII.

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.

Access to PII is role-based and assigned to personnel based on their current job responsibilities. An administratively created account is required to gain access to the stored PII data

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.

Appropriate access is granted to the system based on predefined roles and job descriptions, and administrative access is limited to authorized employees based on current roles.

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.

All employees of IHS and direct contractors are required to complete IHS Security Training and Awareness, IHS Information Systems Security Awareness annual training.

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

All employees of IHS and direct contractors are required to complete HIPAA Privacy, HIPAA Security, Privacy Act Basics, and 42 CFR Part 2 training modules on an annual 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.

This system serves as a secondary repository and is not the official system of record. The primary records are maintained and managed under a separate, applicable records retention schedule. Records maintained within this system are managed in accordance with General Records Schedule (GRS) 5.2-020: Intermediary Records. These records are temporary in nature and will be destroyed upon creation or update of the final record, or when no longer needed for business use, whichever is later.

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

Administrative Controls: All personnel who access IT systems which contain protected information have met background investigation criteria for Public Trust positions. All personnel have taken mandatory security and privacy training classes and annual refreshers. Administrative personnel accessing these systems use privileged and separate accounts for administrative access.

Technical Controls: Access controls lists and event logs are maintained and monitored to detect unauthorized, suspicious or malicious activity. Access lists are restricted to approved IT technical personnel. Two factor authentication must be used for access. File integrity and auditing software are employed on hardware.

Physical Controls: The information technology (IT) hardware used to host protected information is located in a secured IHS facility. The facility is only open to authorized personnel whose access is monitored by locking doors with badge readers for both ingress and egress. Each discrete ingress and egress event is logged. The facility is under 24-hour surveillance by facilities security for security and environmental hazards.