US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

04/21/2026

OPDIV:

IHS

Name:

Nutrition Analysis Program

PIA Unique Identifier:

P-8695353-382970

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 Nutrition Analysis applications enables IHS to deliver nutritionally precise, safe, and culturally appropriate meals for patients, improve operational efficiency, and comply with healthcare and privacy regulations. It functions as a clinical and administrative support tool integral to patient care and dietary management within the IHS healthcare environment.

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

The Nutrition Analysis application used by the Indian Health Service (IHS) supports both patient care and daily hospital operations. It helps staff plan and provide meals that meet each patient’s medical, nutritional, and cultural needs. To do this, the system collects and uses limited information about patients and staff. This information is used only to ensure safe, accurate, and timely dietary services. For patients, the system may collect basic identifying information (PII) such as name, medical record number, date of birth, and location within the facility (such as room or bed number). It also uses health-related information (PHI), such as diet orders (e.g., diabetic, low sodium), food allergies, nutritional requirements, and any dietary restrictions related to medical conditions or cultural

preferences. This information allows dietary staff to prepare meals that are safe and appropriate for each patient.For employees (staff), the system may collect basic PII such as name, employee ID, job role, and login credentials. This information is used to control access to the system and ensure that only authorized staff—such as dietitians, nurses, and food service workers—can view or update patient dietary information. It may also track which staff member entered or updated information for accountability and quality purposes.The system may also store and share operational information, such as meal orders, menu plans, food production details, and delivery schedules. This helps ensure that meals are prepared correctly and delivered to the right patient at the right time. In some cases, limited information may be shared with other internal hospital systems (such as electronic health records) to keep patient dietary information up to date and consistent across care teams.To find or retrieve records, the system typically uses routine identifiers such as a patient's name, medical record number, or room number. For staff, records are usually accessed using employee ID or username. These identifiers help staff quickly locate the correct information without needing to search through unnecessary data.Overall, the system collects only the minimum information needed to safely manage patient nutrition and support hospital operations. All information is protected according to federal privacy requirements, and access is limited to authorized users to ensure patient and staff privacy is maintained.

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

The Nutrition Analysis application used by the Indian Health Service (IHS) is a tool that helps healthcare staff plan, prepare, and deliver meals that are safe, nutritionally appropriate, and culturally relevant for patients. It supports both clinical care and daily food service operations by organizing information about patients' dietary needs and meal services in one place.The system collects and stores information about patients to ensure meals meet their medical and personal needs. This includes basic identifying information such as name, medical record number, date of birth, and location (room or bed number). It also includes health-related details such as prescribed diet (for example, diabetic or low sodium), food allergies, nutritional requirements, and cultural or religious food preferences. In addition, the system may track meal orders, food preferences, and meal delivery information to ensure patients receive the correct meals.The system also collects and maintains information about employees (staff) who use it. This includes name, employee ID, job role (such as dietitian, nurse, or food service worker), and login credentials like username and password. This information is used to control access, ensure only authorized staff can use the system, and track who enters or updates information for accountability and quality purposes.In addition to PII and PHI, the system also handles non-personal operational information. This includes menu plans, recipes, ingredient lists, food production quantities, delivery schedules, and inventory-related details. This type of information helps the facility run efficiently but does not identify any individual on its own. The system may share information internally with other hospital systems, such as electronic health records, to keep patient dietary information accurate and up to date. Information may be stored either temporarily (such as active meal orders) or longer-term (such as dietary history or audit logs), depending on operational and regulatory needs.To routinely find and retrieve records, the system uses specific identifiers. For patients, records are typically accessed using name, medical record number, or room/bed number. For staff, records are accessed using employee ID or username. These identifiers allow staff to quickly locate the correct records while limiting unnecessary access to other information.Overall, the system collects only the information needed to safely manage patient nutrition and support hospital operations. All data is protected and only accessible to authorized users to ensure privacy and security are maintained.

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

Mother's Maiden Name
E-Mail Address
Mailing Address
Phone Numbers
Medical Records Number
Medical Notes
diagnoses, diet orders, food allergies, location within the facility (such as room or bed number), other names, tribe, birthplace, religion, tribal enrollee #, emergency contacts, insurance, outside referrals, mother and fathers name, employer, house location, preferred language, tribal affiliation, other names, Dietary restriction information linked to individuals, Audit logs with user activity, Administrative records tied to individuals, Username /User ID, Employee ID / Badge Number, Role-based access assignments, IP Address Workstation Identifier Session / login timestamps, Encounter/visit number, Admission/discharge dates, Height / Weight / BMI, Nutritional risk score, Privacy complaint records, Security incident / breach documentation, Insurance policy/group numbers, Medicare/Medicaid identifiers, Patient account/billing account numbers, System-generated unique identifiers (GUIDs), Provider identifiers (including NPI)Guardian/responsible party information, Meal selection/tray history, ,Ward/unit/bed transfer history, Consent/acknowledgment records, Backup/archival data copies

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 using PHI and PII in the Nutrition Analysis application at the Indian Health Service (IHS) is to ensure that each patient receives meals that are safe, accurate, and appropriate for their medical and personal needs.For patients, PHI and PII are used to correctly identify the individual and match them with the right dietary requirements. This includes using information such as name, medical record number, and location (room or bed) to make sure meals are delivered to the correct person. Health-related information—such as diet orders, food allergies, and medical conditions—is used to ensure meals meet clinical requirements and do not pose a risk to the patient’s health.For staff, PII is used to manage access to the system and ensure that only authorized personnel can view or update patient dietary information. It also allows the system to track which staff member entered or modified information, supporting accountability and quality of care.Overall, the use of PHI and PII in this system is limited to supporting direct patient care and safe food service operations. It ensures the right meal is prepared and delivered to the right patient, while also allowing staff to perform their duties effectively and securely.

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

Secondary use of PHI/PII in the Nutrition Analysis application at the Indian Health Service (IHS) refers to using patient and staff information for purposes other than directly preparing and delivering meals to an individual patient.While the primary use is to ensure each patient receives the correct diet, secondary use focuses on improving how the system and food service operations work overall. For example, PHI may be reviewed to identify trends in patient dietary needs, such as how many patients require diabetic, low-sodium, or allergy-specific meals. This helps the facility plan menus, manage food inventory, and ensure appropriate resources are available.PHI/PII may also be used for quality improvement activities, such as evaluating whether meals are being delivered on time,

whether dietary restrictions are being correctly followed, or whether documentation is accurate. This supports safer and more efficient patient care.In addition, limited information may be used for reporting, audits, and compliance purposes to ensure the facility is meeting healthcare and federal privacy requirements. Staff PII, such as user IDs and activity logs, may be used to review system access and ensure only authorized users are making changes.All secondary uses are controlled and limited to the minimum necessary information. Where possible, data is summarized or de-identified so that individuals are not directly identified, while still allowing the organization to improve services and maintain compliance.

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

Online

Other

Government Sources

Within OPDIV

Other HHS OPDIV

Other Federal Entities

Identify the OMB information collection approval number and expiration date

N/A. This system is exempt from the Paperwork Reduction Act (PRA) as it Routine clinical care documentation within the agency, where information is collected solely to provide services to patients, not for reporting or regulatory purposes

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.

Memorandum of Understanding (MOU) or Data Sharing agreements are in place to address third-party reimbursement or fiscal intermediary functions for the purposes of billing or collecting third-party reimbursements.

Describe the procedures for accounting for disclosures.

The Indian Health Service (IHS) is required to maintain a record every time it shares a

patient’s personal health information (PHI), noting when the information was shared, what was shared, and why. This requirement applies to disclosures made to business associates, IHS employees who need the information to perform their duties, the patient themselves, federal agencies such as the Department of Health and Human Services when required by law, and other legally authorized disclosures, including those under the Freedom of Information Act or with patient consent. These disclosure records must be kept for at least five years or for as long as the original patient record exists, whichever is longer. Patients have the right to request access to these records to see who has received their information, except for disclosures related to law enforcement under Privacy Act exemptions. If a record is corrected or a note is added due to a patient dispute, IHS must notify anyone who previously received that information, provided a disclosure record exists. To track all disclosures, IHS uses the IHS-505 "Disclosure Accounting Record" form, ensuring that patient information is shared in a safe and legally compliant manner.

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.

Patients and employees have the option to seek healthcare services and employment elsewhere.

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 Health Insurance Portability and Accountability Act (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.

To protect the personal identifiable information (PII) in the system, the program conducts regular reviews of the data to ensure it is accurate, complete, and up to date. These periodic reviews check that the information is correct, available when needed, and relevant for its intended purpose. Any errors or outdated data are corrected, and access is monitored to ensure only authorized staff can view or modify the information. This process helps maintain the integrity, reliability, and proper use of patient data while supporting safe and effective meal planning".

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.

The system provides licenses that allow role based staff to use the program, and these are installed only on computers used by Dietetics department staff and IT department (if needed). Staff access the system using their IHS username and password or a personal identity verification card (PIV). The program also keeps a record of all actions taken in the system to ensure accountability and track usage.

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.

Administrative controls set rules for who can use the system, such as healthcare staff or approved contractors. Physical controls keep the machine and any printed results in secure locations so only those authorized can reach them. Technical controls protect the information inside the machine using passwords, restricted memory, and other built-in security features.

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.

The order will remain in the medical record and be destroyed/deleted 75 years after last episode of patient care or date of death per IHS record retention schedule/disposition authority DAA-0513-2014-0003.

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.