US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

06/02/2026

OPDIV:

IHS

Name:

Medicare Transaction Facilitator Data Module IHS-wide

PIA Unique Identifier:

P-2501299-961277

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)?

Yes

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

Describe the purpose of the system.

The Medicare Transaction Facilitator Data Module (MTFDM) is a Centers for Medicare & Medicaid Services (CMS) system that supports the secure exchange and availability of Medicare transaction and payment-related data. Medicare is a federal health insurance program for individuals age 65 and older and certain younger individuals with disabilities.MTFDM does not perform core IHS clinical or billing functions such as patient registration or claims generation. Instead, it provides IHS users with access to Medicare payment and transaction information to support financial reconciliation and accounting activities. IHS facilities retrieve payment reports from the system to post payments and reconcile billing records within their internal systems.IHS sites do not submit billing or patient data through the MTF portal. The only information uploaded is a site participation authorization form required to establish access. All other system use is limited to viewing and downloading CMS-provided reports.

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

The Medicare Transaction Facilitator Data Module (MTFDM) collects, stores, and shares information needed to process Medicare billing and payments. For patients, this includes personally identifiable information (PII)—information that can identify an individual—such as name, date of birth, email address, address, and Medicare identification number, as well as protected health information (PHI)—health-related information linked to an individual—such as dates of service, medical notes, diagnosis codes, and treatment details used for billing. For staff, the system may include limited PII such as employee names, user IDs, and work contact information to track who enters or processes data. The system uses key data elements like patient name, Medicare identification number, date of birth, and account or claim numbers to routinely retrieve records. In simple terms, the system holds the basic personal and health information needed to bill Medicare and ensures the right records can be found and managed efficiently.

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

The Medicare Transaction Facilitator Data Module (MTFDM) is an Indian Health Service (IHS) system used to support Medicare billing and payment processing. The system collects, stores, and shares information needed to create, submit, and track claims for healthcare services provided at IHS facilities. This includes general administrative data, such as claim numbers, service dates, and billing codes), as well as personally identifiable information (PII) that can identify a person, such as patient names, dates of birth, email address, addresses, and Medicare identification numbers. It also includes protected health information (PHI)—health information linked to an individual—such as diagnoses, procedures, medical notes and treatment details used for billing. For staff, the system maintains limited PII such as employee names, user IDs, and work contact information to manage system access and track actions taken in the system. Some information may be stored temporarily during processing and then transmitted to other systems or Medicare for payment, while other records are maintained for documentation and audit purposes. Records are routinely retrieved using PII data elements such as patient name and Medicare identification number.

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
E-Mail Address
Mailing Address
Medical Notes
Claim or account Numbers, service dates, Medicare identification number, and billing codes
diagnoses, procedures, and treatment details used for billing
user IDs, and work contact information

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 collecting PII that can identify an individual. The Medicare Transaction

Facilitator Data Module (MTFDM) is to ensure that healthcare services provided to patients are accurately billed and paid for under Medicare. The system uses PII to correctly match patients to their Medicare records, create and submit claims, and verify that payments are issued to the appropriate IHS facility. In simple terms, PII is collected so the system can identify the right patient, process billing correctly, and support payment and record keeping for services provided.

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

In addition to billing and payment, the Medicare Transaction Facilitator Data Module (MTFDM) may use PII that can identify an individual for several secondary purposes that support program operations and oversight. These include verifying and correcting billing records, conducting audits and reviews to ensure compliance with Medicare requirements, resolving payment disputes, and preventing or detecting fraud, waste, and abuse. The information may also be used for reporting and analysis to improve financial management and healthcare operations within the Indian Health Service (IHS). In simple terms, beyond getting claims paid, the information helps ensure accuracy, accountability, and proper management of Medicare-related activities.

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.

09-70-0500 – “Medicare Enrollment Database (EDB), Medicare Beneficiary Database (MBD), and

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

Hardcopy

Email

Online

Government Sources

Within the OPDIV

Other OPDIV

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 Health Insurance Accountability and Portability 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.

The Medicare Transaction Facilitator Data Module (MTFDM) uses routine checks and reviews to make sure personally identifiable information (PII)—information that can identify an individual—remains accurate, complete, and available when needed. Staff regularly review records during normal billing and reconciliation activities to confirm that patient and claim information is correct and up to date. The system also supports audits and monitoring, where authorized staff compare data against source records and correct any errors found. Access controls and system backups help ensure the information is protected and available, while outdated or unnecessary information is handled according to records retention policies. In simple terms, the system relies on ongoing staff review, system checks, and established policies to keep information accurate, relevant, and accessible.

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.

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.

Note: web address is a hyperlink.