US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

02/06/2026

OPDIV:

CMS

Name:

MedTrak

PIA Unique Identifier:

P-3267375-367468

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.

PIA Validation

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

Not applicable

Describe the purpose of the system.

MedTrak is an Enterprise Tracking System Application developed to support all aspects of the Clinical Data Abstraction Center (CDAC) contract: Medical Abstraction, Validations, and Reporting.

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

MedTrak collects medical records which may include Social Security Numbers, Driver's License Number, Mailing Address, Device Identifiers, Mothers Maiden Name, Medical Record Number, Patient Name, E-mail Address, Phone Numbers, Medical Notes, Date of birth, Date of Death, Therapy Records, and Patient x-rays.

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

MedTrak is an expansive workflow system which allows Clinical Data Abstraction Center (CDAC) to receive, abstract, validate, process, report, and destroy records for our contractual obligations.

PII is retrieved from the database and shown to the abstractor at the start of abstracting a record to verify they have the correct patient and dates of service.

The MedTrak is the Clinical Data Abstraction Center Enterprise Tracking System being implemented to collect medical records or information from Quality Improvement Organizations (QIOs) or hospitals as part of the Clinical Data Abstraction Center (CDAC). MedTrak is responsible for processing over 80,000 medical records per year. MedTrak is designed to request, store, and retrieve medical records for use in medicals studies. The studies are created and managed through various agencies within the government. MedTrak is the workflow, which includes tracking and operational system used by CDAC to perform abstraction and validation of the medical records. The work conducted by the CDAC is finalized in the Inpatient Perspective Payment System (IPPS) final rule which is a requirement of the statute finalized by congress.

With MedTrak, we are validating provider reported quality measure outcome data by reviewing the medical record, and performing medical record reviews for healthcare related adverse events. It is not only important to make sure that the data received by Centers for Medicare & Medicaid Services (CMS) is a quality data but it is a mandatory requirement based on the statute finalized by congress. Based on the information gained by collecting/abstracting/validating medical records CMS is able to keep the providers accountable for not only providing quality data but also improving the overall care provided to the CMS beneficiaries in the participating hospitals across the nation. This perhaps helps save lives with good quality of care.

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
Date of Death
Therapy records

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

Patients
Patients, Physicians, Physician Groups, Dialysis Facilities, Hospitals, and Outpatient Providers.

How many individuals' PII is in the system?

100,000-999,999

For what primary purpose is the PII used?

The PII is used for Medical Abstraction, Validations, and Reporting

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

The Personally Identifiable Information (PII) is used for Testing, Training, and Research

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

Medicare Improvements for Patients and Providers Act (MIPPA), 2008.

2008, E.O. 9397

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.

Published: Medicare Beneficiary Database (MBD), HHS/CMS/CBC 09-70-0536

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

Other

Non-Governmental Sources

Identify the OMB information collection approval number and expiration date

Other

Not applicable

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.

Individuals are notified by their healthcare provider that their information can be shared for providing healthcare services, payment, and validation/auditing/fraud prevention.

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.

MedTrak can receive PII from two groups: the medical providers and their patients. Medical providers' contact information such as name, address, phone number, and email address can exist in MedTrak. Medical providers are not required to provide all of this information (voluntary), and it is not required for MedTrak's operation. For patients, sensitive personal information, such as name, address, and phone number, are requested by medical providers to patients at the time of treatment. Also, medical record data is collected on patients as a part of treatment. When medical providers transmit medical records to CMS MedTrak, sensitive personal information may be embedded in the medical record. While the presence of sensitive personal information to MedTrak users is not typical, it can exist and without specific patient’s consent. CMS does not provide an "opt out" option to patients. There are no civil or criminal penalties for a failure to provide PII as this information is not required for MedTrak's operation.

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

There is no process to notify individuals. There is a process to notify CMS if disclosure is necessary.

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.

CDAC has no role directly with patients and this would need to take place with CMS or the provider.

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 MedTrak system employs a partnership of trust with its data sources.

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.

CMS has a standard process to vet MedTrak users and its development team. All MedTrak users have received authorization from CMS to access the system and its Personally Identifiable Information/ Protected Health Information (PII/PHI).

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.

MedTrak operates under least privilege principles and does not allow users to search by name.

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 MedTrak users sign a Memo of Understanding; Rules of Behavior; and Privacy Agreement. Rules of Behavior and Security Awareness training are required to be completed annually.

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

All abstractors go through multiple training for each of the different modules in which they work.

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.

Disposition Authority: N1-440-09-3

General Records Schedule Number DM-0440-2015-0008

MedTrak uses CMS Bucket 6 – Provider and Health Plan Records for the General Record Schedule and is located at the following URL: https://www.cms.gov/Regulations-and-Guidance/Guidance/CMSRecordsSchedule/Downloads/Bucket-6-Provider-and-Health-Plan-Records.pdf. However, MedTrak is not the system of record for the medical records that it consumes, and, therefore, the system does not retain PHI for the seven years noted in the General Record Schedule.

PII Retention

PHI and PII in MedTrak are located in consumed medical records. The medical records are received digitally into the AWS S3 bucket, users analyze and validate them, and records are retained in the system for approximately 6 months. After the retention period ends, the data is deleted using the AWS S3 rules for data destruction.

The retention duration is configurable and managed in the Project Administration Application of MedTrak. In cases of an exception – such as an appeal, education review, or quality assurance – a medical record can be retained separately in a “Hold” state for a longer period of time, as needed to complete the exception operation.

For any maintenance tools that may retain information, the ADO follows CMS procedures which comply with NIST SP 800-88 to sanitize the tools prior to dispositioning or modifying the use of the tool.

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

Administrative controls:

MedTrak inherits CMS policies and AWS procedures and capabilities for securing PII/PHI. MedTrak users are trained each year on proper handling of business sensitive, PII, and PHI data. MedTrak complies with the Privacy Act of 1974 by allowing only authorized individuals to access PII and by protecting the use, transport, and storage of PII and PHI in accordance with CMS policies. MedTrak minimizes the storage of PII/PHI and only accesses and uses PII/PHI in accordance with the CMS data abstraction requirements and authorization. In alignment with CMS governance and policies, data fields are categorized to define which are PII and PHI to maximize masking when possible. MedTrak creates data logs that can be monitored and analyzed for inappropriate access and use.

Technical controls:

All PII/PHI is encrypted when stored and in transit in MedTrak. MedTrak restricts and masks fields as appropriate. For data in transit, MedTrak encrypts using TLS 1.2 to service endpoint. For data at rest, MedTrak uses AWS KMS (SSE-KMS) S3 encryption. Data is encrypted using FIPS 240-2 compliant technology.

Physical controls:

Users’ computers are secured using automatic logouts and timed sleep modes. Computer access is only available with biometric multi-factor authentication. Users only see PII/PHI data on a need-to-know basis, and access to the data is tracked in MedTrak logs. All PII/PHI is maintained within the protected CMS VPN and AWS environments.