

# US Department of Health and Human Services

## Privacy Impact Assessment

**Date Signed:**

03/16/2016

**OPDIV:**

CMS

**Name:**

Medicare Administrative Issue Tracker and Reporting of Operations

**PIA Unique Identifier:**

P-8632397-077943

**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.**

The Medicare Administrative Issue Tracker and Reporting of Operations (MAISTRO) initial Authority to Operate(ATO) was granted in 2008 and has been renewed thereafter. In April 2013, the application was moved to an Internet URL --which was NOT accessible by the public -- from a CMS intranet URL following a successful and independent Security Controls Assessment and receipt of a renewed Authority to Operate (ATO). As of 8/28/2015, MAISTRO is no longer accessible via the Internet; instead, MAISTRO now uses a CMS Intranet URL. Only

users with an approved CMS User ID and MAISTRO-specific job codes can access MAISTRO; the general public can NOT.

**Describe the purpose of the system.**

MAISTRO serves as a CMS inquiry management tool to ensure CMS accountability for responding to Medicare fee-for-service inquiries from the public. It is a repository for Medicare Part A and Part B inquiries directed at CMS plus documentation of CMS's responses to those inquiries. The system also provides data for reports that track workload and emerging trends within the fee-for-service program.

The MAISTRO system records and tracks Medicare beneficiary and provider inquiries and complaints through to their resolution. MAISTRO provides detailed reporting functionality related to pending and closed inquiry records for CMS analysts' individual workload data as well as for regional or nationwide Medicare issue data.

The reporting functions allow for many standard and ad hoc reporting options critical to managing the inquiry workload of the CMS Consortium for Financial Management and Fee for Service Operations (CFMFFSO), including timeliness calculations for CMS responsiveness to congressional offices and other inquirers; workload volumes by component or inquiry category; FFS trends and emerging issues; and inquiries related to new programs or initiatives.

The reporting outputs do not contain PII or PHI unless an analyst specifically must search for such data (e.g., to locate historical information about a caller's Medicare issue or prior assistance that CMS provided).

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

The MAISTRO system provides a resource for CMS to store Medicare beneficiary and provider inquiries and complaints and to document CMS actions in response to those inquiries. Information collected in MAISTRO may include name, address, date of birth, Medicare number or Health Insurance Claim Number (HICN), e-mail address, and phone number.

Information provided by an inquirer will vary depending on what is needed to research and resolve the particular complaint or inquiry.

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

MAISTRO documents inquiries submitted to CMS by beneficiaries, congressional offices, providers, and others regarding Medicare Parts A and B (fee-for-service or 'traditional' Medicare), including Medicare Electronic Health Records (EHR) and ACO (Accountable Care Organization) inquiries.

Analysts from CMS's Central and Regional Offices enter information into MAISTRO related to each inquiry, including attachments such as scanned incoming correspondence and CMS responses, and they document actions taken to resolve and respond to each inquiry.

The system was designed to allow limited use by other CMS-affiliated individuals with valid CMS User IDs (e.g., grantees or contractors) to document their Medicare related inquiry workloads in the system, but this option has never been used and is not currently being used. Only CMS employees use MAISTRO and enter with a username and password and MAISTRO is accessible only through a CMS Intranet URL.

The MAISTRO system records and tracks Medicare beneficiary and provider inquiries and complaints through to their resolution. The information collected for the MAISTRO functions described may include beneficiary and/or provider name, address, date of birth, HICN, e-mail address, and phone number, depending on what is needed to research and resolve the particular complaints or inquiries.

**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

Phone Numbers

Health insurance claim number (HICN); Provider number

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

Employees

Public Citizens

Business Partner/Contacts (Federal/state/local agencies)

Vendor/Suppliers/Contractors

Congressional inquirer contact info, providers and suppliers (doctors, hospitals, facilities, etc.)

**How many individuals' PII is in the system?**

100,000-999,999

**For what primary purpose is the PII used?**

The data are collected from individuals who proactively contact CMS for assistance with their Medicare fee for service issues, and any data collected are for the purpose of helping those individuals resolve their Medicare concerns.

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

In limited instances, CMS may rely on geographic information from MAISTRO to analyze whether a local or regional issue is occurring (for example, a lack of availability of providers or durable medical equipment), or similar types of trending analysis may be done to determine if education or outreach is needed about a Medicare matter for beneficiaries or providers.

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

Authority for maintenance of this system is given under § 923 of the Medicare Prescription Drug, Improvement, and Modernization Act of 2003 (MMA) (Public Law (Pub. L.) 108–173) which created the Office of the Medicare Ombudsman.

**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.**

Medicare Administrative Issue Tracker and

**Identify the sources of PII in the system.**

**Directly from an individual about whom the information pertains**

In-Person

Hardcopy

Email

Other

**Government Sources**

Within OpDiv

Other HHS OpDiv

State/Local/Tribal

Other Federal Entities

## **Non-Governmental Sources**

Public

### **Identify the OMB information collection approval number and expiration date**

Individuals are not required to provide information. If an inquirer seeks CMS assistance with Medicare-related inquiries, they may choose to provide sufficient information so that the inquiry can be researched and resolved by CMS.

### **Is the PII shared with other organizations?**

Yes

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

#### **Within HHS**

Two CMS systems (NGD-Next Generation Desktop and NDW-National Data Warehouse) associated with 1-800-Medicare. Certain 1-800-Medicare inquiries that must be resolved by a CMS subject matter expert are routed to the appropriate CMS office through MAISTRO rather than by email or fax, etc.

#### **Other Federal Agencies**

CMS analysts may need to communicate PII to such agencies (such as Social Security) in order to obtain resolution of a Medicare issue for an individual.

#### **State or Local Agencies**

CMS analysts may need to communicate PII to such agencies (such as a state Medicaid office that pays for an individual's Medicare premiums) in order to obtain resolution of a Medicare issue for an individual.

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

Memorandum of Understandings (MOUs) are in place. MAISTRO data are accessible to CMS staff to allow responses to Medicare Part A, Medicare Part B, HITECH, and ACO inquiries or complaints from the public. Under limited circumstances and pursuant to an Interface Control Document, limited data are shared with two other CMS systems associated with 1-800-Medicare to facilitate resolution of 1-800-Medicare call center inquiries that CMS must resolve. Those two CMS systems are the National Data Warehouse (NDW) and the Next Generation Desktop (NGD). they are owned and managed by another CMS office (OTS).

### **Describe the procedures for accounting for disclosures.**

If disclosure of PII is necessary to assist a

Medicare beneficiary in resolving a Medicare issue or problem, CMS analysts typically communicate about this with the inquirer seeking the assistance. Progress Notes or Resolution Notes within MAISTRO can be used to document communications. MAISTRO has Data Use Agreements (DUAs) in place which documents the data being disclosed, who it is being disclosed with, for what purpose, and for what time frame.

The business purpose of MAISTRO is to track inquiries and requests that arrive at CMS from a variety of sources while providing staff with a standardized tracking system so they may account for and resolve those requests accurately and promptly. The individuals who seek CMS assistance may supply their PII in order for CMS to research and resolve their complaints which at times requires involvement of another agency (e.g., Social Security or a state Medicaid office).

The analyst would take notes and document who the disclosure is made with, when it was made and for what purpose which will be entered within the MAISTRO case record.

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

Consent for collecting PII is implied when individuals initiate contact with CMS and ask for assistance with resolving issues with their Medicare entitlement, provider enrollment, or other similar matters which CMS has a duty to resolve. Collection of PII is inherent in the verbal intake process (if CMS receives the inquiry by phone or the inquirer presents in person) or such information may be provided by the inquirer proactively via correspondence (email, mail, fax). Individuals are not required to provide their name, health insurance claim number, birthdate, provider number, etc., but if such information is needed to assist the individual, CMS staff may not be able to provide the requested service without it.

**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.**

Depending on the issues presented, PII may be necessary for CMS to offer assistance and resolution. Whenever individuals contact CMS for assistance, they always have the right to decline to give any personally identifiable information. However, without such information, in some instances CMS's assistance may be limited if it precludes the necessary research and analysis.

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

Such major system changes that would impact PII use or disclosure will be published in the Federal Register as part of a modification of the MAISTRO System of Record Notice (09-70-0598). If any changes were to occur to MAISTRO which would impact the reasons for the original data collection and disclosure, a revised SORN would be published to the Federal Register for a 60-day period for public review/comment.

**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.**

Medicare.gov, 1-800-MEDICARE, and HHS.gov Office of Civil Rights sites are available for reporting allegations of violations of collection and/or disclosure of PII.

**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 MAISTRO Data Quality Workgroup, comprised of CMS MAISTRO users, performs routine sampling of MAISTRO records to provide continuous improvement opportunities for CMS analysts on various quality measures including a means to contact individuals (such as name and telephone or e-mail address) who request assistance from CMS. The workgroup also reviews outcomes as reported by analysts to ensure accurate issue resolution, which requires relevant, accurate information.

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

**Users:**

To record details of new fee-for-service inquiries as they occur and to document CMS actions taken in response to the inquiry. Individuals are also allowed to update existing inquiries.

**Administrators:**

Only CMS employees with valid CMS User IDs are permitted to have the MAISTRO system administrator role, which is dependent upon an approved job code. This role is limited to application-specific functions, managing inquiries, and assisting users; it does not control access to the system.

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

MAISTRO is a CMS application, so all users must first meet the stringent criteria for obtaining a CMS User ID. MAISTRO is also a role-based application, and a System Administrator must approve each request to access MAISTRO and each specific role requested. Only upon being granted access to MAISTRO will a user be able to view PII, and for many roles that view is limited to the component within which the employee works.

**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.**

As a role-based application, MAISTRO has built-in functional limits based on which role a user is

permitted by a System Administrator. The roles are authorized based on a user's job requirements and each role provides various levels of access to MAISTRO screen views, data fields, search and report options.

**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 MAISTRO users must first have a valid CMS User ID, and to obtain a CMS User ID, an individual must complete an online security-based training managed by CMS. To retain a CMS User ID, that training must be completed annually. Security and Privacy Act topics about protecting PII and PHI are included in such training. Also, upon requesting access to CMS systems, a user must read and attest that he or she will comply with all CMS security requirements. A user is also presented with a warning statement and rules of behavior upon each attempt to access MAISTRO, and the user must affirmatively agree to comply with these before being given access to the system.

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

In addition to completing mandatory annual security and privacy training to retain his or her CMS User ID, MAISTRO users are provided additional training on such topics in periodic User Group meetings several times each year.

**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.**

MAISTRO will follow the current CMS Records Schedule retention policies as approved by the National Archives and Records Administration (NARA). Specifically, Disposition Authority: N1-440-04-3 ; Disposition Authority: N1-440-10-5, Item 8; Disposition Authority: N1-440-07-1, Item 9; Disposition Authority: N1-440-10-6 which states to destroy 5 years after the date of the response to the correspondence, or when no longer needed for Agency business, whichever is longer, Item 1; Disposition Authority: N1-440-10-6, Item 2 which states destroy 2 years after the date of the response to the correspondence, or when no longer needed for Agency business, whichever is longer; Disposition Authority: N1-440-10-6, Item 3 which states to destroy 2 years after the date of the response to the correspondence, or when no longer needed for Agency business, whichever is longer. 3. Inquiries /Correspondence - No Response Required; Disposition Authority: N1-440-10-6, Item 3 which states to destroy 3 months after the date of the incoming correspondence, or when no longer needed for Agency business, whichever is longer.

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

All data are secured in accordance with CMS controls within the guarded, locked, CMS Baltimore Data Center and as described in the MAISTRO Systems Security Plan (SSP). Only individuals who have current CMS User IDs and

passwords and who obtain pre-approved specific role-based job codes are authorized to access MAISTRO. All such users must complete annual training on CMS security and privacy policies and must adhere to them. Protections are in place to prevent misuse of a user's ID and password (e.g., lock out after failed access attempts). MAISTRO also undergoes the annual FISMA security controls testing and complies with all other CMS security activities required to maintain the CMS Chief Information Security Officer (CISO) Authority to Operate (ATO).