US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

10/21/2016

OPDIV:

CMS

Name:

Measure Authoring Tool

PIA Unique Identifier:

P-9261213-845342

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?

Yes

Identify the operator.

Contractor

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.

Quality measures are tools that help measure or quantify healthcare processes, outcomes, patient perceptions, and organizational structure and/or systems that are associated with the ability to provide high-quality health care and/or that relate to one or more quality goals for health care. These goals include: effective, safe, efficient, patient-centered, equitable, and timely care.

The Measure Authoring Tool (MAT) provides measure developers with the ability to compose and export electronic Clinical Quality Measures (eCQM) in the Health Quality Measures Format (HQMF), including human readable and simple Extensible Markup Language (XML) formats. The MAT supports the authoring of eCQMs that are able to be expressed using the Quality Data Model. Measures may be process measures or outcome measures. The MAT can support development of measures for scoring types such as: Proportion, Ratio or Continuous Variables.

The MAT is an open source system designed and maintained in partnership with various stakeholders, including, but not limited to, Centers for Medicare & Medicaid Services (CMS), Health Care Innovation Services (HCIS), Value Set Authority Center (VSAC), Enterprise Science and Computing (ESAC), and MITRE, to become the standard under which eCQMs are built and are defined for use in governmental and non-governmental systems. Electronic measure creation and maintenance requires the use of Value Set information that is provided through MAT integration with the National Library of Medicine (NLM) Value Set Authority Center (VSAC).

The Measure Development Community is tasked with authoring and maintaining electronic Clinical Quality Measures (eCQMs) for a variety of public and private initiatives. Measure Developers may be contracted to perform measure development and maintenance on behalf of CMS or another agency. In turn, these measures are included in programs and policy that utilize quality measurement.

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

The MAT collects information about persons. The information is collected via the User Registration Form, the MAT Login page, and via the Contact Us page of the MAT website.

The system collects First Name, Last Name, Middle Initial, Personal Address(including City, State, and Zip Code), Business Email (may potentially be personal email address), Business Phone Number (may potentially be personal phone number), and Business Name for the purpose of account administration and collaboration between measure developers. Authorized system administrators and help desk personnel access the data for the purpose of account administration and correspondence.

Registrants are required to have their MAT Registration Form notarized by providing their MAT Registration Form and a government issued photo ID to a Notary Public. The Notary uses a government issued photo ID to verify the identity of individuals by ensuring the information on the ID corresponds to the information provided in the MAT Registration Form. The MAT system does not make copies of ID's, nor does it store, or maintain them.

The MAT user ID is provided to MAT users via email. MAT user IDs, account passwords, and multifactor authentication security codes are collected for identification, authentication and access management purposes, when logging onto the MAT system.

The system discloses PII to authorized help desk and program personnel for the purpose of sending e-mail notifications regarding system changes and system status.

The system discloses PII to the registered users for the purposes of sharing measure definitions.

In the normal course of business, the MAT does not share PII with external entities. In the event user interactions indicate evidence of criminal activity, a threat to the government, or a threat to the public, PII may be shared with appropriate agency officials or law enforcement.

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

The MAT consists of:

A public website at www.emeasuretool.cms.gov;

A production Measure Authoring Tool environment for measure development, where registered users build and export standardized measure definitions for use in other systems (Note: The MAT only builds definitions for measures; however, the MAT does not actually compute the measures or access any data that is used to compute a measure.)

The MAT is designed to allow electronic Clinical Quality Measure (eCQM) developers to compose eCQM logic and export eCQMs in Health Quality Measures Format (HQMF),
human readable, and Simple Extensible Markup Language (XML) formats. eCQM composition requires the use of Value Set information that is provided through MAT integration with the National Library of Medicine (NLM) Value Set Authority Center (VSAC).

There are 2 types of PII collection for the MAT:
The system collects the following information for the purposes of account registration and identity proofing at an eAuthentication Level 2 for the Measure Authoring Tool: First Name, Last Name, Middle Initial, Personal Address (including City, State, and Zip Code), Business Email (may potentially be personal email address), Business Phone Number (may potentially be personal phone number), and Business Name.

This information is shared with system administrators for the purpose of establishing a user account in the Measure Authoring Tool. This information is stored outside the web site.
The system uses First Name, Last Name, Middle Initial, Business Email (may be a personal email address), and Business Name for the purposes of establishing an account in the Measure Authoring Tool.

This information is shared with authorized system administrators for the purposes of managing a user's account in the Measure Authoring Tool. E-mail address is shared with authorized system administrators, authorized program managers, and authorized MAT Help Desk personnel for the purpose of sending email notifications regarding account status changes and changes to the MAT system. First Name, Last Name, and Organization are shared with other registered MAT users for the purpose of sharing measure definitions, and for providing a history of changes to measure definitions.

The system collects Name and Email to respond to questions or comments submitted through the email link on the Contact Us page of the web site.

This information is shared with the MAT Help Desk and authorized program personnel for the purposes of responding to the individual's inquiry.

The MAT user ID is provided to MAT users via email. MAT user IDs, account passwords, and multi-factor authentication security codes are collected for identification, authentication and access management purposes, when logging on to the MAT system.

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

Yes

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

Name

E-Mail Address

Mailing Address

Phone Numbers

User ID, password, zip code

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

Employees

Public Citizens

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

How many individuals' PII is in the system?

100-499

For what primary purpose is the PII used?

Individuals must provide their PII for the setup and maintenance of their individual accounts to respond to questions or comments submitted through the email link on the Contact Us page of the web site.

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

Not applicable.

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

Affordable Care Act, Section 3021 is the legal authority governing information use and disclosure specific to the system and program.

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.

The Privacy Act System of Records Notices (SORN) used by MAT are SORN 09-70-3005

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

Hardcopy

Email

Online

Government Sources

Within OpDiv

Non-Governmental Sources

Public

Identify the OMB information collection approval number and expiration date

MAT is exempt from needing an OMB information collection approval number per the Medicare Access and CHIP Reauthorization Act of 2015 (MACRA) legislation.

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.

A Privacy Policy link is provided at the bottom of each page of the public web site and within the Measure Authoring Tool. (https://www.emeasuretool.cms.gov/web/guest/ privacy-policy)

The privacy policy includes a link to http://www.usa.gov/optout-instructions.shtml, which provides instructions on blocking cookies.

Individuals are instructed to contact the MAT Help Desk with any questions or concerns regarding the privacy policy.

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.

The collection and use of PII in the Measure Authoring Tool only pertains to users of the system and is required for the purposes of account registration and management.
Therefore, there is no option for users to opt- out of the collection of their user ID and password as it is necessary to perform their job. Use of the Measure Authoring Tool is voluntary.

The privacy policy includes a link to http://www.usa.gov/optout-instructions.shtml, which provides instructions on blocking cookies.

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

A Privacy Policy link is provided in the footer of each page of the public web site and within the Measure Authoring Tool. (https://www.emeasuretool.cms.gov/web/guest/ privacy-policy)

The following actions are taken to notify individuals of any changes to the privacy policy:
A News and Alerts message is posted on the public web site.
Email notifications are sent to registered users of the Measure Authoring Tool
Privacy policy is updated on the public web site.

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.

Individuals are instructed to contact the MAT Help Desk with any questions or concerns regarding the privacy policy. Individuals are provided with a contact person through the SORNs who will address their concern and triage as necessary.

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

As PII is related to accounts for registered users, PII is checked for accuracy as part of quarterly account audits.

E-mail bounce back messages trigger a review of relevant accounts.

MAT system maintainers have implemented both unique and regular indexes to support data integrity and prompt data retrieval. Data is encrypted at rest, which supports data integrity. Data access is limited to system administrators and end users with authorized access.
Logs are maintained to track any changes made to data that include who modified a particular file and when those changes were made. The data sets used by the MAT are under the purview of the CMS Data Integrity Board.

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

Users:

For purpose of sharing measure definitions with other users.

Administrators:

For purpose of administering accounts of registered users and for issuing email notifications.

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

Administration of the system is divided between development, test, and production systems.

MAT system design, development, and support staff must have their access approved by the MAT system owner, before being provided access to the MAT system and system information.

Developers do not access production systems. Administration is separated by duties. Separate personnel administer servers, network, and applications with only the rights necessary to carry out assigned duties. Within the application, role base access is utilized to assure users have access to only what is necessary to perform their specific requirements.

MAT Registration Forms are processed and stored in a locked cabinet, where access is provided to only support staff that requires access for the processing of user registration.

MAT Registration Forms are maintained for at least two years, and are shredded upon disposal.

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.

Access to PII is restricted by role based access controls to authorized personnel, who are provided the minimum necessary access to perform the job functions of the individual’s assigned role.

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.

MAT system design, development, and support staff are required to take CMS privacy and security training prior to initial system access and annually for continued access to MAT Application data.

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

Not applicable.

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.

Account registration and corresponding accounts for the measure authoring community are retained in accordance with General Records Schedule (GRS) 3.2 Information Technology and Management Records DAA- GRS-2013-0006-0003, "Destroy 1 year(s) after user account is terminated or password is altered or when no longer needed for investigative or security purposes, whichever is appropriate."

System audit logs retained in accordance with General Records Schedule, Electronic Records GRS 4.3, item 020, "Delete/destroy when the agency determines they are no longer needed for administrative, legal, audit, or other operational purposes."

Retention policies are in line with the NARA guidelines outlined in N1-GRS-03-1 which states, "Destroy/delete when 5 years old or 1 year after responsible office determines that there are no unresolved issues, whichever is longer. (N1-GRS-03-1 item 1a)."

Data destruction policies follow NIST guidelines provided in NIST Special Publication 800-88 Revision 1, Guidelines for Media Sanitization.

Electronic records such as passwords are cleared from the system when changed. End of life hard drives and paper records are destroyed via a certified and bonded shred company.

Electronic records are purged. Paper records are destroyed via a certified shred company.

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

Technical controls include but are not limited to:
Authorized users: Unique identification and password authentication for access Measure Authoring Tool.

Separation of duties, filters and parameters are set up in accordance with an approved configuration to enforce the security policy.

Data back up on a daily and weekly basis, with the weekly tapes going off-site for storage.
Destruction of electronic information, as appropriate, via sanitation of the systems holding the information.

Audit of events initiated by each individual user, i.e., entry of User ID and password, program initiation, file creation, file deletion, file open, file close, and other user related actions,
Audit trails identify the individual user initiating the event, date, and time the event occurred, success, or failure of each event, and location where the event was initiated.

Physical controls include but are not limited to:
Building access cards and ID badges are required in the main facility and only authorized personnel have access to the locked data center where the hardware used to process this system data is located.

Security guards are present during working hours and off-hour visits are made by security personnel. Closed-circuit television (CCTV), is used for monitoring of the facility. Back up media is stored offsite in a secure, climate controlled storage facility. Visitor process includes signing in and out, visitor badges and escorting of all visitors. Uninterruptible Power System (UPS) with a diesel generator back up to ensure ongoing system operation and an orderly shutdown when necessary.

Power to the data center is separated from the power to the rest of the facility and additional heating, ventilating, and air conditioning (HVAC) with humidity controls is in place. Locked shred bins are utilized for document and media destruction and certificates of destruction are received from the bonded destruction company upon completion.

Administrative Controls include:
Procedural safeguards: Users must comply with terms of use to reinforce the confidentiality protection requirements, and the confidentiality policy is reviewed and signed on an annual basis.

Security training and ongoing awareness programs, such as posters and newsletters. Access controls, including termination procedures to ensure only authorized personnel have access to facilities and systems, commensurate with their job duties.

Review of system activity logs to monitor for issues, Risk Management plans to include Risk assessments, Security Plans, Continuity of Operations/Disaster Recovery plans. Background and reference checks are performed on all HCIS personnel.

Identify the publicly-available URL:

https://www.emeasuretool.cms.gov

Note: web address is a hyperlink.

Does the website have a posted privacy notice?

Yes

Is the privacy policy available in a machine-readable format?

Yes

Does the website use web measurement and customization technology?

Yes

Select the type of website measurement and customization technologies is in use and if it is used to collect PII.

Session Cookies that do not collect PII.

Persistent Cookies that do not collect PII.

Does the website have any information or pages directed at children under the age of thirteen?

null

Does the website contain links to non- federal government websites external to HHS?

No

Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?

null