Modified EP/EO Determination System (MEDS) – Privacy Impact Assessment

Approved Sept. 11, 2008

System Overview

The Tax Exempt Determination System (TEDS) provides the foundation and infrastructure for MEDS and was designed to correct existing severe shortcomings, it is also necessary to support new requirements of the major strategies and operational priorities defined in TE/GE's Strategic Plan. The initial TEDS scope was to address other key shortcomings in future releases. Since the final release of TEDS is expected December 2008, there will be a number of functionalities that will need to be addressed. MEDS is expected to take up where TEDS leaves off and deliver other key functionality in releases slated for July 2008 through March 2009.

System of Records Numbers

- [Federal Register: December 7, 2005 (Volume 70, Number 234)]
- Treasury/IRS 34.037 – IRS Audit Trail and Security Records System
- Treasury/IRS 50.222 - Tax Exempt/Government Entities (TE/GE) Case Management Records

Data in the System

For compliance with Executive Office of the President – OMB Memorandum M-07-06 dated May 22, 2007, Safeguarding Against and Responding to the Breach of Personally Identifiable Information and to Reduce the Use of Social Security Numbers; the MEDS Applications have been reviewed for their use of social security numbers to identify instances in the collection or use of the social security number, see attachment. All MEDS Data collection has been implemented with alternatives to agency use of Social Security Numbers as a personal identifier for both Federal employees and as identifiers for Agency Applicants.

1. Describe the information (data elements and fields) available in the system in the following categories:

A. Taxpayer

MEDS includes information relating to an organization and/or employee plan, which is used to determine whether or not the organization and/or employee plan is eligible for tax-exempt status. MEDS uses Employer Identification Number, (EIN), for Application Owner, which is stored within the MEDS Data base, as provided on hard copy applications and supporting documentation received from an organization, which are submitted to the TE/GE office for a determination of the tax exempt eligibility of an organization and/or employee plan. Submitting applicants should already have an EIN.

MEDS does not capture Individual Social Security numbers. In rare circumstances, it is possible that an individual taxpayer may supply their SSN on an application for determination of a plan. If a SSN is supplied, upon receipt of an application with a SSN, the case specialist would ensure that the EIN, and not SSN, had been entered as case data, and make any necessary changes. Also, the case image with the SSN would be transferred from the Disclosable to Non-Disclosable folders within the case; limiting the permissions of some MEDS users to view that document. Only the Employer Identification Number (EIN) is tracked as the identifier in the MEDS database and the only presence of the SSN would be in the image stored on a series of servers at the ECC-MEM in Memphis, which is accessible to high level System Administrators at the TCC, and to certain TEGE EO & EP MEDS users, based on assigned roles and responsibilities.

The taxpayer information collected will be taken from a variety of applications, and Power of Attorney Forms 2848 and Form 8821. Power of Attorney information may be written in a free-flow format. This information is then manually entered into the system. Other forms utilized include Forms 1023 and all its associated schedules (which uses 417 barcode scan to convey information), 1024, 1026, and 1028 for exempt organization entries and Forms , 5300, 5303, 5307, 5309, 5310, 5310A, and 5316 for employee plan entries. Through an automated process the information from these forms are entered into the computer. There is generic information on all forms; however, not all information is required for each form as the forms or application serve different purposes.

Typical information may include:

- Plan Sponsor Name
- Employer Identification Number
- Plan Name
- Address to include City, State, and Zip Code
- Telephone Number (Business)
- Person to Contact for more information, to include Name and address
- Name of Employer
- Employer's tax year end (Month)
- Details of the plan to include funds returned to the employer, proposed plan termination, plan type, membership in controlled groups, reason for termination, funding arrangement
- Name of Trustee(s), telephone number and address.
- Number of participants in the plan and statistical information
- Employer contribution and forfeitures
- How distribution will be made upon termination
- Receivables, general investments, employer related investments, building and other property used in plan operation, benefits claims payable, operating payables, acquisition indebtedness, and other liabilities
- Signature and title of Employer
- General Eligibility Requirements
- Date incorporated or formed
- Number of shares of current outstanding capital stock and other details
- Value of agricultural products
- Gross dues
- Expenditures such as Compensation of officers, directors and trustees, other salaries and wages, Interest, Rent, Dues and assessments of affiliated organizations, etc.
- Assets
- Liabilities and Capital

B. Employee

Employee data used in this system consists of profile information that is stored and used to route work to the employee (e.g., User Identification (SEID) group number), access limitations).

IRS employee information included in the MEDS application is information used to identify the user/IRS employee processing the claim and includes:

- Employee name
- Employee user ID
- Employee's manager name
- Employee's manager user ID
- Employee Contact Information (address and phone number)

C. Audit Trail Information

MEDS maintains an application audit trail (also known as case chronology). Scanning auditing is conducted through use of Captiva (COTS software), this auditing of users is conducted at the GSS level after each of the following actions:

- Scan
- Package review module checks contents of package (QA step)
- Image quality assessment (skew, de-skew)
- Pages are identified for OCR (based on form)
- Package submission
- OCR is performed
- These audit records are stored in a proprietary database using InputAccel, and may only be viewed by privileged managers with access to the Manager's Console.

Following an audit triggered by Captiva, Documentum (COTS software) maintains a log of all database activity.

The MEDS Documentum application audit trail includes the following information:

- Successful Logons or logoffs
- Unsuccessful logons
- Change Of Password (use of identification and authentication mechanisms)
- Data files opens and closed (Introduction of designated objects into a user's address space)
- Specific Actions, such as reading, editing, deleting records or fields within Open and Closed Cases
- Creation, modification and deletion of designated objects
- Change in access control permissions
- User annotations made for each access or change made to the case
- Startup of a TEDS application component
- Running/Printing/Updating Reports
- Audit Log starting and stopping
- Audit Log Full
- Audit Log Purge
- All SA actions while logged on as a SA
- Batch file modifications to database
- Direct manipulation of records in the database and bypassing TEDS
- Date
- Time (to the nearest second)
- User SEID
- Data Component where event occurred
- Type of Event (User, File or other resource affected)
- Action Taken (IP Address, System name)
- Case Number
- Disabled Auditable Events
- System Administrator Actions
- Added User
- Subject Identity (SEID, Group, Phone Number)
- Outcome of Event (success/failure)
- Unique identifier for each transaction (User Name, SEID, Application Name)

- Status_Code (effected by update)
- CASE_NUMBER (MEDS Case Number)
- DATE_CHANGED
- DATE_ENTERED
- USR_CODE (single MEDS User ID from Captiva)
- COMMENTS

D. Other (Describe)
No other information is used in the MEDS.

2. Describe/identify which data elements are obtained from files, databases, individuals, or any other sources.

A. IRS
Technical specialists may query the Business Master File (BMF), Employee Plans Master File (EPMF), National Account Profile (NAP), and Certified Authorization File (CAF) "Power of Attorney" mainframe system to verify information contained in an organization's application. However no information from the BMF, EPMF, or NAP is stored on MEDS.

Payment status information on applications is supplied by the IRS Letter Information Network User System (LINUS).

B. Taxpayer
Information stored within the MEDS is provided on hard copy applications and supporting documentation received from an organization, which are submitted to the TE/GE office for a determination of the tax exempt eligibility of an organization and/or employee plan.

C. Employee
The functional security manager is responsible for adding the SEID of users into Documentum. MEDS compares the SEID of the user's account to the SEID which was added into Documentum. The SEIDs must match for access to Documentum to be granted. IRS LAN accounts are created at the GSS level.

D. Other Federal Agencies
Currently no Federal Agencies provide data for use in MEDS.

E. State and Local Agencies
Currently no State or Local Agencies provide data for use in MEDS.

F. Other third party sources
Currently no other third party sources provide data.

3. Is each data item required for the business purpose of the system? Explain.
Yes, each data item is required in order for IRS employees to determine if an organization meets all requirements for exemption or to determine if an employee plan is a qualified employee plan.

4. How will each data item be verified for accuracy, timeliness, and completeness?
Captiva is used for scanning and imaging all correspondence. Optical Character Recognition (OCR) is used to convert the hard copy text into a soft copy. MEDS users at the CSPC then use Captiva FormWare to correct and validate the data. The technical specialist will review each application for sufficient data necessary to scan the document. Automated business rules check to ensure information is complete and will cite what information might be missing. The technical specialist reviews the business rules findings and makes the final determination on completeness and can overrule the business rules if necessary.

5. Is there another source for the data? Explain how that source is or is not used.
No, MEDS does not collect information from sources other than IRS records or taxpayers.

6. Generally, how will data be retrieved by the user?
The user will retrieve information from MEDS through a Web-based interface using the organization's EIN or a number assigned to uniquely identify each application in MEDS (the MEDS Case Number).

7. Is the data retrievable by a personal identifier such as name, SSN, or other unique identifier?
Yes, MEDS data can be retrieved by EIN, name, or MEDS Case Number.

Access to the Data

8. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Others)?
MEDS does not allow access to the public. Personnel who will have access to data in MEDS:

- IRS Determination workload managers.
- IRS Determination reviewers and managers.
- IRS Determination agents/technical specialists.
- Customer account service representatives.
- Documentum Database Administrator.

Contractors who might require access to the data are required to have a full background investigation and complete the OL5081 process and receive manager's approval before performing any MITS activities through MEDS.

9. How is access to the data by a user determined and by whom?
Access to data within the system is restricted through settings on Documentum and Captiva. Restrictions are based on business rules contained in the MEDS Business Rules Document. Documentum designates 8 different levels of access permission, while Captiva strictly allows or disallows a user access. MEDS uses roles and privileges to control the levels of access a user account may have. In general, managers can do anything the people they manage can do.

A user's position and need-to-know determines the level of access to the data. The System Administrator grants approval for system access. A user's access to the data terminates when the user no longer requires access to MEDS.

The following mandatory rules are defined for users of all IRS computer and information systems:

Users are forbidden to access, research, or change any account, file, record, or application that is not required to perform official duties.
Users are restricted to only accessing, researching, or changing accounts, files, records, or applications that are required to perform their official duties. Access is limited by the users' role and assignments. MEDS does not interface with the User TIN list.
Users are restricted from accessing their individual/spouse account, accounts of relatives, friends, neighbors, or any account in which the user has a personal or financial interest. Users are restricted from accessing the accounts of famous or public persons unless given authorization.
If asked to access an account or other sensitive or private information, users are required to verify that the request is authorized and valid. Users will be held accountable if they access an unauthorized account.

Users are required to retrieve all hard copy printouts in a timely manner, ensure that magnetic media is secured based on the sensitivity of the information contained, and that they will practice proper labeling procedures. Users are instructed not to disclose or discuss any IRS-related information with unauthorized individuals.
Users are instructed to protect IRS employee internal work from disclosure.
All vendors are to be escorted and monitored.
The user's access will be restricted by the access limitations assigned to the profile associated with the user's unique USERID. The profile is established to allow workflow activities to route documents and cases to the proper specialists.

Profiles are assigned by MEDS Functional Security Managers. The Functional Security Managers periodically review the roles to ensure that user authorizations are correct. There are three MEDS Functional Security Managers for each organization and they participate in the OL5081 process.

10. Do other IRS systems provide, receive, or share data in the system?
MEDS communicates with Letter, Information & Network User Fee System (LINUS).

The exchange of information between LINUS and MEDS begins with new applications (both remit and non-remit) being entered into LINUS. Once the application information has been entered into LINUS, and the payment/check has been removed from the application package, the application package is sent to document preparation and scanned into the Receipt and Handling subsystem. The package will remain in Receipt and Handling until LINUS reconciliation occurs.

LINUS will provide MEDS with user fee information for the application after completion of the batch reconciliation process for new applications (initial user fees) and established cases (additional user fees). After the LINUS user fee reconciliation process, MEDS will complete the application verification steps, process the user fee information from LINUS, and send LINUS the application related data that LINUS requires.

11. Have the IRS systems described in Item 10 received an approved Security Certification and Privacy Impact Assessment?
Yes, LINUS has an approved security certification and approved Privacy Impact Assessment.

12. Will other agencies provide, receive, or share data in any form with this system?
Internal Revenue Code §6104(c)(A) requires that IRS notify "the appropriate State officer" of a Denial or Failure to Establish issued to an organization that applied for recognition of exemption under §501(c)(3), or of a Termination by a §501(c)(3) organization. To meet this requirement, on a monthly basis MEDS generates a paper list of Denials, Failures to Establish, and Terminations, which are then mailed to the respective states with a Memorandum of Understanding with the IRS. For each entity the list includes the name, address and EIN. The states do not maintain any direct access to the MEDS database, nor is any data transmitted electronically.

Administrative Controls of Data

13. What are the procedures for eliminating the data at the end of the retention period?
Information will be retained for ten years and EO determination information will be retained indefinitely. (EO Administrative Case Files are included in IRM 1.15.36, Records Control Schedule for Permanent Records.)

14. Will this system use technology in a new way?
No

15. Will this system be used to identify or locate individuals or groups?
No

16. Will this system provide the capability to monitor individuals or groups? If yes, describe the business purpose for this capability and the controls established to prevent unauthorized monitoring.
Yes. Office of Foreign Asset Control (OFAC) monitoring capabilities will be included in MEDS.

17. Can use of the system allow IRS to treat taxpayers, employees, or others, differently?
The system does not make allowances for different treatment as a standard business process, however, the system does allow certain cases to be expedited (by Congressional or Executive Order or the Department Head) only if cases are approved. Otherwise, the first and default priority for handling cases is the post-mark date.

18. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action?
Yes. For a "negative determination" as to exemption/qualification, the applicant is notified of a proposed adverse determination and is given an opportunity to protest before any final action is taken. Additionally, the applicant has the right to go to Appeals (or EO Technical or EP Exam for certain cases).

19. If the system is Web-based, does it use persistent cookies or other tracking devices to identify Web visitors?
MEDS does not use persistent cookies or other tracking devices to identify Web visitors. Documentum allows users to make use of a persistent cookie if they so choose, but does not set this cookie as a default setting. There is no password information (only SEID) retained in the cookie. If the user chooses to use the cookie, it is stored on their computer and is protected under the user profile to prevent other users from accessing that cookie.

View other PIAs on IRS.gov