LSDM Privacy Impact Assessment Sample Form

1. **OPDIV:**
CMS

2. **PIA Unique Identifier (UID):**
TBD

    a. **Name:**
    LSDM Data Repository and Analytical Tool

3. **Which of the following objects does this PIA cover?**
Major Application

    a. **Identify the Enterprise Life-Cycle Phase of the System:**
    Development and Testing

    b. **Is this a FISMA Reportable System?**
    Yes

4. **Does the system include a publicly available Web interface?**
    Yes

5. **Identify the operator**
    Contractor, Optimal Solutions Group, LLC

6. **Is this a new or existing system?**
    New

7. **Does the system have Security Authorization (SA)?**
    No

    a. **Date of Security Authorization**
    TBD

    b. **Planned date of Security Authorization**
    September 2015

    c. **Briefly explain why security authorization is not required.**
    NA

8. **Indicate the following reason(s) for updating this PIA. Choose from the following options:**

NA

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

NA

10. Describe the purpose of the system.

Fulfill Government Performance and Results Act (GPRA) reporting requirements and gain efficiencies by providing a secure, online application to collect, store, and report on learning activity data across CMMI innovation model and provide real-time access to the Agency and model learning system contractors.

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

(Subsequent questions will identify if this information is PII and ask about the specific data elements.)

The system will collect and maintain data on learning events, participant organizations attending events, individual participants attending events. Optimal is collecting individual participant data that consist of participant names, business e-mails, organization affiliation, and the participant's role within an organization. Most of the data collected is publicly available and considered contacts management information.

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

- The goal of LSDM is to collect data regarding learning events in order to track the various activities of the learning events. Over time, the aim is to correlate the levels of engagement in learning activities with model outcomes.
    - Events are the main unit of analysis.
    - Events are broken down by event type, which includes model-specific event type, cross-model event type, event purpose, post-event survey information etc.
- Each learning system has a model contractor, from whom Optimal receives monthly learning event data.
- Contracts for the learning system model contractors have been modified, which permits them to submit to the Learning Systems Data Management Contractor the learning event data that they collect.
- The purpose of collecting individual participant data is to map participants, and their roles, to events within and across models to examine how participation in learning events impacts outcomes within the models.
- The system will provide access to model contractors to enter and edit their own learning activity data and to view a dashboard summarizing their compliance and performance in relation to overall performance across model. CMMI will have access to compliance and performance information for each model and across models.

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

Yes. However, most of the data collected is publicly available and considered contacts management information.

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

Name
Business email address

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

Public Citizens
Business Partner/Contacts (Federal/state/local agencies)
Vendor/Suppliers/Contractors:
Other: Employees, partners, consultants of organizations participating in CMS innovation model projects or demonstrations.

16. How many individuals' PII is in the system?

17. For what purpose is PII used?

To identify key players in an organization implementing a CMS innovation model and their participation in learning activities to be able to correlate that participation with model outcomes.

18. Describe secondary uses for PII which will be used (e.g. testing, training or research)

Feedback to model contractors on learning activity attendance and learning system improvement.

19. Describe the function of the SSN.

NA

20. Cite the legal authority to use the SSN.

NA

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

Government Performance and Results Act (GPRA) of 1993 and GPRA Modernization Act of 2010

22. Are records on the system retrieved by one or more PII data elements?

Yes

23. 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.

No SORN number yet.

SORN is in progress.

24. Identify the OMB information collection approval.

NA

25. Identify the sources of PII in the system.

a. Non-Government Sources
b. Other: CMS model learning system contractors

26. Is the PII shared with other organizations?

No

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

NA

b. Describe any agreements in place that authorizes the information sharing

NA

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

Event participants are not officially notified that their personal information is collected for the purposes of Government Performance and Results Act (GPRA) reporting. However, event participants provide their information when they register for or login into (in the case of virtual events) learning events. They have a general understanding that their information may be used for attendance reporting purposes in the context of the model learning system. The Learning System Data Management effort is obtaining the information from the model learning system contractors that host events.

28. Is the submission of PII by individuals voluntary or mandatory?

Voluntary

29. Describe the method for individuals to opt-out of collection or use their PII. If there is no option to object to the information collection, provide a reason.

If the learning event requires registration/login, an individual must provide a name and email to access the online portion of the event or attend an in-person event. For online events, the individual could provide a false name and email if they do not want to provide

their real name and business email. If participants only access the teleconference portion of a virtual event, no PII is requested. For in-person events, real names and email must be provided so that travel and event logistic information can be provided. In-person event participants are not provided an option to object to the data collection, but there is a general understanding that their information may be used for attendance reporting purposes in the context of the model learning system.

30. Describe the process to notify and maintain consent from the individuals whose PII is in the system.

All major system changes concerning personally-identifiable information (PII) are published for comment in the Federal Register as part the applicable System of Records Notice (SORN).

31. 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. If no process exists, explain why not.

An individual record subject who wishes to know if this system contains records about him or her should write to the system manager who will require the system name, and for verification purposes, the subject individual's name and organization.

An individual seeking access to records about him or her in this system should write to the system manager and reasonably specify the record contents being sought. (These procedures are in accordance with Department regulation 45 CFR 5b.5 (a) (2).)

To contest a record, the subject individual should contact the system manager, and reasonably identify the record and specify the information being contested. The individual should state the corrective action sought and the reasons for the correction with supporting justification.

System Manager:

32. Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy. If no processes are in place, explain why not.

The system has a transactional audit trail that will record changes to data over time and produce reports that show those changes. Further, participant records are assigned unique IDs based on name and email combination to prevent duplicate records. As new event records are added, the system will recognize participants based on name and email combination. Participant records are also entered through a form or uploaded via a

template with built in quality control checks that will flag invalid email addresses or possible duplicates.

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

a. User Check Box: Yes
b. User Reason: Model learning system contractors will only have access to the participant data they have collected and entered into the system.
c. Administrators Check Box: Yes
d. Administrator Reason: Administrators will have access to PII for analysis and reporting.
e. Contractors Check Box: Yes
f. Contractors Reason: The Learning System Data Management (LSDMC) Contractor, is building the system and executing all LSDM reporting. They require access to for reporting, quality control, and execution of security controls.

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

The access rights are controlled by the privilege assigned to the user role. Contract staff members who are involved in data analysis are required to undergo role-based security awareness training.

35. 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.

PII is safeguarded by Federal Information Security Management Act (FISMA) and National Institute of Standards and Technology (NIST) requirements and protocols. Access to PII is limited to the users that provide PII, who only have access to the PII they provide and system administrators for reporting and quality control. Additionally, researchers granted access to the data collected do not have administrative access to the underlying hardware or software environment, in accordance with NIST Special Publication 800-53 rev.4 AC-5 [“Separation of Duties”], AC-6 [“Least Privilege”].

36. 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.

Annual Privacy and Security Training required of all federal contractors. All Learning System Data Management contractors undergo role-based security awareness training, in accordance with NIST Special Publication 800-53 rev.4 AT-3[“Role Based Security Training”] and PS-5 [Personnel Transfers].

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

Once the system is operational users will be trained on how to enter and edit data in the system and run the reports they have access to or view and navigate their customized results dashboard.

38. Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices.

Yes

39. Describe the process and guidelines in place with regard to the retention and destruction of PII. Cite specific records retention schedules.

The records will be stored in the system, which will reside in a secure Federal Risk and Authorization Management Program (FedRAMP) –approved environment, for the duration of the Learning System Data Management contract with Optimal Solutions Group. Upon contract end, all records will be transited to CMMI and all copies destroyed, the database deleted, and the server reformatted and wiped clean. The current contract fourth option year ends August 2019.

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

Administrative controls: Management oversight of activities, security awareness and training for users of the system and role-based training for administrators and others with privileged access, and execution of contingency plans and business continuity exercises.

Technical controls: Separation of duties for personnel administering the system, isolating development, test, and production instances of the system, and Secure Socket Layer (SSL) for browser to server communication. User authentication (login) and logical access controls, anti-virus software, Operating System Patch Management, intrusion detection, fire walls, and role-based access through the database application. The database is behind a fire wall to protect it from web intrusion. Password complexity requirements for all user accounts. Password clipping levels established to lock accounts that use incorrect password more than 5 times.

Physical controls: Server housed in secure facility, climate control, fire alarm, fire extinguishers and Uninterrupted Power Supply (UPS) for servers.