US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

02/22/2016

OPDIV:

CMS

Name:

Medicare Learning Network Learning Management and Product Ordering System

PIA Unique Identifier:

P-7025219-203713

The subject of this PIA is which of the following?

Major Application

Identify the Enterprise Performance Lifecycle Phase of the system.

Planning

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.

null

Is this a new or existing system?

New

Does the system have Security Authorization (SA)?

No

Indicate the following reason(s) for updating this PIA.

New PIA

Describe the purpose of the system.

MLN REPOS is the system that hosts all MLN web-based training (WBT) courses, allows learners to voluntarily register for those WBTs, print their certificates of completion, and order hardcopy MLN products. This system is available to the general public and is designed for CMS program health care professionals.

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

MLN REPOS collects and stores Medicare health care professional transcript/certificate data for MLN WBT courses. This data includes information pertaining to the health care

professional (name, phone, address, email address, health care provider type, health care facility type, and professional association affiliation). Users will register online and also assign their own login ID and password. These will be used to access their account. This information is not shared with any other systems and is only accessible to administrators (which are both Centers for Medicare & Medicaid Services (CMS) employees and CMS contractors). No one, including administrators, has access to a learner's password.

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

MLN REPOS is a voluntary system that collects and stores Medicare health care professional transcript/certificate data for MLN WBTcourses in order to track training course completion. This data includes information pertaining to the health care professional (name, phone, address, email address, health care provider type, health care facility, and professional association affiliation). System Users (healthcare professionals, CMS employees and CMS contractors) will register online and also assign their own login ID and password. These will be used to access their account. This information is not shared.

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

Certificates

User ID and password, Health Care Provider Type, Health Care Facility Type,

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

Employees

Public Citizens

Vendor/Suppliers/Contractors

How many individuals' PII is in the system?

100,000-999,999

For what primary purpose is the PII used?

Name, Mailing Address, and phone number are collected due to CMS' requirement as a continuing education provider. Since we offer continuing education credit for our web-based trainings (WBTs), we are required to collect this information. Email addresses are collected so that we can easily find account information for learners who contact us via our email resource box for assistance. Health Care Provider Type, Health Care Facility Type, and Professional Association affiliation are collected to inform us about our audience and make future marketing and product development decisions. Users will register online and also assign their own login ID and password. These will be used to access their account. None of the PII data is shared.

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.

Title IV of the Benefits Improvement Protection Act of 2000 (Public Law (Pub. L.) 106–554, Appendix F), Title IV of the Balanced Budget Act of 1997 (Pub. L. 105–33), and §§ 1816(a) and 1842(a)(3) of the Social Security Act.

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: 2007-03-08

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Online

Government Sources

Within OpDiv

Non-Governmental Sources

Public

Identify the OMB information collection approval number and expiration date

Not applicable. This is not necesary since the system is only collecting registration information, which is Paperwork Redemption Act (PRA) exempt.

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.

The user chooses to enter their personal information in order to create an account in the system. Creating an account is voluntary.

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.

Individuals can choose to opt-out of the collection of their PII by choosing not to create an account in our system.

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

No major changes have occured to the system to necessitate notifying and obtaining consent from the individuals whose Personally Identifiable Information (PII) is in the system. However, if necessary, notices can be sent via email address to the individuals to notify them and obtain consent.

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 an individual believes their PII has been inappropriately obtained, used or disclosed, or if their PII is inaccurate, they can contact our resource mailbox at MLN@cms.hhs.gov. These inquires will be handled by CMS administrators. If an individual believes their PII has been inappropriately obtained, used or disclosed, this will be investigated. If an individual believes their PII is inaccurate, instructions will be given on how they can correct this within the MLN REPOS system.

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

Our system contractor maintains the data

integrity and availability by employing security procedures including firewalls and encryption layers. The users of the system and CMS administrators maintain data accuracy and relevancy. Users can correct their own PII data within their own account, or administrators can correct this for them if they are alerted to changes. Administrators also run monthly reports and will see an discrepancy or problems with data integrity, availability or accuracy and take necessary action to remediate.

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

Administrators:

Administrators require access to they can locate and search for learner accounts to assist with questions or issues.

Contractors:

The contractor that owns and maintains the system has access so they can test and update programming. They only access learner account/PII information when the administrators run across a system issue with an account that the contractor must resolve.

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

The MLN REPOS administrator, who is a CMS employee, determines which CMS employees have access to PII based on their need to know in order to perform their job functions. Only those who will be working within MLN REPOS and answering our resource box are given administrative access and access to PII.

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.

MLN REPOS automatically assigns the general user role when a user creates an account. This allows the user to only view their own information and account after they login using their login ID and password. If more access is needed, the MLN REPOS administrator will assign the appropriate system role to the CMS employee user to allow them access for need to know information to complete their job functions. MLN REPOS has several system roles that can be used to limit administrative access to specific areas of the system, such as just content administrative access for those updating course material or just learner account access for those assisting learners. If a user has any system role other

than the basic user role, they will be required to enter their login ID and password and also a unique alphanumberic code that is emailed to them each time they login.

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 administrators are CMS employees or CMS contractors, and therefore have completed the annual CMS Information Systems Security Awareness and Privacy computer-based trainings.

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

Administrators undergo training with the Administrator Lead before they are given responsibilities within the system. They review the administrator processes which discuss the proper use and disclosure of PII. They are reminded that PII should be protected and not shared.

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.

Per SORN 09-70-0542 (title: MLN Registration and Product Ordering System): "The records are maintained online in the system for 8 years. After an 8-year period, the records are transferred to an inactive file and destroyed 2 months later." Additionally, NARA General Records Schedule (GRS) 24 states that the records will be destroyed/deleted when records are inactive six years after user account is terminated or password altered, or when account it no longer needed for investigative purposes.

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

For administrative controls, a CMS staff member is not approved as an administrator with access to PII unless it is determined by the Lead Administrator and Technical Lead that the access is necessary for the employee to complete their job duties. Multi-factor authentication (If a user has any system role other than the basic user role, they will be required to enter their login ID and password and also a unique alphanumberic code that is emailed to them each time they login) is also in process for administrators that will further protect

access to this information. Technical controls include the firewall and encryption protections in place within the system to secure PII. Physical controls include security and monitoring of the servers and data center at our system contractor's site.

Identify the publicly-available URL:

https://learner.mlnlms.com

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.

Other technologies that do not collect PII:

Base code

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

No

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