US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

03/14/2016

OPDIV:

OS

Name:

Think Cultural Health

PIA Unique Identifier:

P-2321544-798208

The subject of this PIA is which of the following?

Minor Application (stand-alone)

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?

Existing

Does the system have Security Authorization (SA)?

No

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.

None

Describe the purpose of the system.

The Think Cultural Health (TCH) website provides tools and resources to promote cultural competency in health care. The site can be used as a resource (researching information on cultural competency) and/or a source for e-learning continuing education units (CEU) for health care professionals. Health care professionals can enroll online and successfully complete the various cultural competency modules. Health care professionals elect or volunteer to complete the educational programs as participation is not mandatory. In order to receive CEUs, the health care professional is required to register online and provide the following information: username, password, first name, last name, highest degree earned, certificate type, address, city, state, zip code, country, sex, age, ethnicity, race, primary language, how well English is spoken, job type, primary place of employment, level of seniority, how did they learn about Think Cultural Health, would they like to join the Centers for Linguistic and Cultural Competency in Health Care (CLCCHC), how did they hear about National CLAS Standards and contact in the future about this program.

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

Think Cultural Health collects the names and contact information for individuals that use the system to receive training and education. Also, as part of the contractual requirement to Office of Minority Health (OMH), bi-yearly evaluation reports are produced that provide information on the number of users per curriculum; how many CEUs have been granted; what the course completion rate is per program, etc. As part of that analysis, the contractor includes a breakdown of users by gender, age group, and other data elements, as defined below, to understand the user community, and to target appropriate outreach activities, if necessary. In these reports, this information is presented in the aggregate and is not broken down by individual. Data elements collected include: user-name, password, first name, middle initial, last name, degree, certificate type, address, city, state, zip code, country, sex, age, nationality, race, primary language, how well English is spoken, professional role, primary place of employment, professional seniority, how did you hear of this e-learning program, would you like to join the Center for Linguistic and Cultural Competency in Health Care, heard about Culturally and Linguistically Appropriate Services (CLAS) Standards, and contact in the future about program experience. Users submit these data elements/personal identifying information (PII) voluntarily, but it is necessary for them to provide it to provide them with proper credit and verification of training received.

User credentials for system developers are stored through the Active Directory Website. Website credentials for system administrators, staff, and public users are stored on the TCH website database. Public users create accounts to take the educational courses and obtain continuing education credits. No reports are created or maintained for system administrators, contractors, or staff.

The data collected from the TCH database is transmitted via zipped and encrypted email to the following accredited agencies: Cine-Med and Indian Health Services. The accreditation agencies aggregate the data and create reports. The reports are then distributed to the healthcare licensing bodies for consideration of credit for relicensing purposes. The reports created for contractual requirements to the Office of Minority Health (OMH) do not contain PII and are statistic based reports on cumulative numbers. The TCH reports are stored at the TCH development center in Reston, Virginia on a network attached storage (NAS) device.

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

The Think Cultural Health (TCH) website provides tools and resources to promote cultural competency in health care. The site can be used as a resource (researching information on cultural competency) and/or a source for e-learning continuing education units (CEU) for health care professionals. Health care professionals can enroll online and successfully complete the various cultural competency modules. Health care professionals elect or volunteer to complete the educational programs as participation is not mandatory. In order to receive CEUs, the health care professional is required to register online and provide the following information: user-name, password, first name, last name, highest degree earned, certificate type, address, city, state, zip code, country, sex, age, ethnicity, race, primary language, how well English is spoken, job type, primary place of employment, level of seniority, how did they learn about Think Cultural Health, would they like to join the Centers for Linguistic and Cultural Competency in Health Care (CLCCHC), how did they hear about National CLAS Standards and contact in the future about this program.

User credentials for system developers are stored through the Active Directory Website. Website credentials for system administrators, staff, and public users are stored on the TCH website database. Public users create accounts to take the educational courses and obtain continuing education credits. No reports are created or maintained for system administrators, contractors, or staff.

The data collected from the TCH database is transmitted via zipped and encrypted email to the following accredited agencies: Cine-Med and Indian Health Services. The accreditation agencies aggregate the data and create reports. The reports are then distributed to the healthcare licensing bodies for consideration of credit for relicensing purposes. The reports created for contractual requirements to the Office of Minority Health (OMH) do not contain PII and are statistic based reports on cumulative numbers. The TCH reports are stored at the TCH development center in Reston, Virginia on a network attached storage (NAS) device.

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

Education Records

Employment Status

Nationality

Sex

Race

Age

Primary Language

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

Employees

Public Citizens

Vendor/Suppliers/Contractors

Users interested in continuing education courses offered through website. These include doctors, nurses, emergency technicians, first responders and other health professionals. Public citizens although some are (coincidentally) Federal workers.

How many individuals' PII is in the system?

100,000-999,999

For what primary purpose is the PII used?

The information is used to enroll individuals and deliver training and education to them; to provide information required to receive and maintain site accreditation from the accreditor, Cine-Med; to provide reports on the use of the system as described above; and to contact interested parties with information about programs in which they may be interested. Office of Public Health and Science (OPHS) and OMH authorized staff use the data collected to call users' attention to OMH programs of interest, report continuing education fulfillment to Cine-Med (the accrediting agency), as required by subpoena, court order or other legal process, and provide products or services requested by the user. The site can be used as a resource (looking up information on cultural competency) and/or a source for e-learning continuing education credits.

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

Not Applicable. PII is not used for secondary purposes.

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

It supports the Office of Minority Health within the Office of the Secretary of the Department of Health and Human Services (HHS/OS/OMH) in complying with the cultural competency requirements of the Patient Protection and Affordable Care Act of 2010 (ACA) (P.L.111-148, see especially Section 5307: Cultural Competency, Prevention, and Public Health and Individuals with Disabilities Training), as well as the Secretary’s Plan to Reduce Racial and Ethnic Health Disparities, the National Stakeholder Strategy for Achieving Health Equity, Healthy People 2020, the Secretary’s Strategic Plan priorities, and the Assistant Secretary for Health’s Public Health Quality agenda.

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.

Think Cultural Health, 09-90-1202

Identify the sources of PII in the system.

Online

Government Sources

Within OpDiv

Non-Governmental Sources

Public

Private Sector

Identify the OMB information collection approval number and expiration date

OMB No. 09-90-1202, expiration date 04/30/2016

Is the PII shared with other organizations?

Yes

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

Within HHS

The information is only shared within the Department of Health and Human Services (HHS), specifically Office of Minority Health (OMH) and, for accreditation purposes of the Disaster Preparedness website (a sub-domain of TCH), Indian Health Services.

Private Sector

OPHS/OMH authorized staff use the data collected to
a) report continuing education fulfillment to the accrediting agencies.
b) as required by subpoena, court order or other legal process
The private sector includes the accrediting agency, specifically Cine-Med, who manages and approves the continuing education requirements for online education sites for health care continuing education accreditation. This reporting is required to maintain accreditation status and standings.

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

As the continuing education accrediting agency, the recipient has a legal/statutory right to the data collected for continuing education licensing requirements and information is used to ensure correct reporting of continuing education units to the accrediting agency. No other agreements are executed.

Describe the procedures for accounting for disclosures.

The Think Cultural Health website policy for routine and non-routine disclosures (see http://www.justice.gov/opcl/privstat.htm for more details) is covered in the Think Cultural Health

Websites Security Plan under Section 8 Privacy & Confidentiality. Adherence to the Privacy & Confidentiality Policy is covered in Rules of Behavior Policy & Confidentiality Agreements (signed by all employees). Failure in the procedure for accounting of non-routine disclosures is addressed in the Incident Response Plan and reviewed yearly in the Incident Response Plan table top tests.

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

On every new or edited registration form, a notification is present describing the process of collecting personal information as well as a Privacy Statement is included on every website. The information includes Privacy Act of 1974 information as well as information that furnishing the information requested on the registration form is optional and the purpose for which the information is used (to administer the Think Cultural Health training programs) and that contact information is used to ensure correct reporting of continuing education units to the accrediting agency and all other information is used to compile statistics about users of the site.

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 are aware of what information is being collected because they choose to supply it themselves, on a voluntary basis. There is further information in the link to the OMH privacy policy at the bottom of each web page as well as a notification on every new or edited registration form, describing the process of collecting personal information.

Individuals know how their information will be used because it is optional to register and use the e-learning/newsletter, to enroll in online courses and receive information.

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

No major changes to the system that would affect individuals' rights and interests are anticipated, but if there were such changes, individuals would learn of them through changes in the SORN, or if necessary, could be informed via the contact information they supply when registering for online educational courses (phone and e-mail).

This is not a mandatory program. Users can choose to opt out of program participation and any future emails.

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.

Contact email links are provided that go to the technical help desk and are answered within 24 business hours.

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 Think Cultural Health website is provided as an e-learning tool and information is collected directly from the website registrants/users by completing a universal online website registration form used by all individuals who wish to register to receive a monthly newsletter through the site or to complete training offered on the site. Information being collected is voluntarily provided by registrants/users. This site is offered to interested parties as a service, and is not updated because the receipt of the benefit (e-learning/receiving information) of the system does not necessarily depend on accurate information; or, if proof of completion is needed, people benefiting from the system will be responsible for making sure their information is entered accurately (and can correct or update it). Processes are in place to assure that PII is reviewed and maintains its integrity, availability, accuracy and relevancy. Monthly scanning is performed that technically challenges the database. Hackers pose tremendous risks to web applications and it's content. For example, they can manipulate a web application in an attempt to inject their own SQL commands into those issued by the database thus changing a user's data, Monthly tests are performed on the TCH system with automated vulnerability scanning and manual vulnerability scanning to determine any weak areas for hackers to access the data. If issues are found, the issues are investigated, remediation completed, and tested prior to the next round of monthly tests. Access to the production environment is limited to only those who require access, and in the case of the developers/engineers who are assisting with trouble shooting issues, the access must be requested, approved then logged. The information is available to users at any time and they have the ability to alter their own registration information (for example in the case of a misspelled word) whenever they need. The content of the registration questions and the course content are reviewed yearly for relevancy and updated as needed. File back ups are tested monthly to ensure that the content is available and the integrity of the data is in tact. Only those users who are on the help desk or data analytics teams can access the Administrative tool, which allows viewing of aggregate or individual data. Website users who elect to complete the TCH programs register themselves and can edit the registration data themselves. The PII entered by the user is validated only by the specific field for the database entries. Fields may be masked for specific purposes such as a date field or a free text field. For example, the user cannot enter alphabets in a date field. As this is an ongoing training course, and users can stop and start the course at any time (even years later), no data is deleted.

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

Administrators:

Access to Administrators Tool for reporting/data collection and for trouble shooting help desk inquiries

Developers:

Database access for reporting/data collection and for trouble shooting help desk inquiries

Contractors:

Database access for reporting/data collection

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

Only those users with Administrative authorization and have been approved to create a username and password are authorized to access PII. Administrative authorization is limited to select group of individuals who work on the Think Cultural Health project and also work on the help desk support team or the data analytics team. The Think Cultural Health technical project manager individually invites the help desk support person or data analytics team member to register for access to the Administrative tool. An email is sent to the team member that includes a token to create their own password for the Administrative tool. No other users, including the technical project manager has access to the passwords created for the Administrative tool. The passwords are stored in the TCH database and are encrypted. The developers only have database access when trouble shooting help desk issues are needed. The developers are required to send the technical project manager and system administrator an email indicating the need for database access and the reason. The request is reviewed and if determined that access is needed, the access is granted. As soon as the issue has been resolved, the database access for that developer is revoked and access to the database and revoking of access is logged in the live database file.

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.

The Administrative tool is used to allow the least amount of access to the authorized user at the time of set up. The rights to access the Administrative tool is limited and only those people who are on the help desk team or the data analytics team are granted access to the data available in the Administrative tool. When the user is invited to register for the Administrative tool, the technical project manager creates the user in the Administrative tool and an email token is sent to the user to create their own password. At the time the technical project manager enters the new username in the Administrative tool, the technical project manager determines the access points needed to that user based on their job role. For example, there is one access point that is only available to the technical project manager and that is for the adding of users to the Administrative tool. Only the technical project manager has the ability to add new users to the Administrative tool. The access points granted to the help desk team and data analytics team are aggregate reports and individual reports.

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.

Each employee undergoes yearly Learning Management System (LMS) training including Information Security Awareness, Privacy Awareness and Role Based Training.

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

Each employee must sign Confidentiality agreements and the Think Cultural Health team conducts yearly table top tests and policy and procedure reviews.

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.

The National Archives and Records Administration (NARA) retention schedule for this system is as follows:
Records Schedule Number: DAA-0514-2013-0002
Disposition Authority Number: DAA-0514-2013-0002-0001
Retention period: Destroy/delete 6 years after the discontinuance of the system. Also, the accreditation of elearning continuing education credits (Cine-Med) requires retention for 6 years after discontinuance of the system)

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

TCH uses the technical, operational, and physical security controls as required by the National Institute of Standards and Technology (NIST) guidance in order to minimize the overall risk to PII. If a security incident does occur, it will be immediately reported to the Chief Information Security Officer (CISO) and then to the Department of Health and Human Services (HHS) Privacy Breach Response Team. They will analyze the incident, determine its impact, limit its damage, and restore normal processing.

Administrative controls include going through the OS Cybersecurity Certification and Authorization process yearly, including Authority to Operate review. Also included is yearly auditing by the OS Cybersecurity team, and the TCH System Security Plan is updated yearly, including all the required supporting documentation. TCH stringently follows a File Back Up Plan where the Web servers and media servers are backed up daily using incremental backups. Full backups are performed every two weeks. Backups are performed to tape. Every six weeks, tapes are overwritten and every sixth month, tapes are grandfathered. All databases are backed up daily and transaction logs are backed up every 15 minutes to disk on a separate server. Transaction logs are kept for two days on the servers. Full database backups are moved off site every night to the development center and stored on disc. Every month, those backups will be archived to tape and kept for two years.
For training, all staff complete yearly LMS training including Information Security Awareness, Privacy Awareness and Role Based Training as well as additional training. Contractors adhere to privacy provisions and practices. All contractors complete LMS training including Information Security Awareness, Privacy Awareness and Role Based Training as well as additional training such as Incident Response Plan review and table top tests yearly. Only specific employees are permitted access to the production and staging server databases and administrative tools. Access to production servers are granted by the technical project manager and system administrator on a case by case basis, and all grants are logged. PII retention and destruction: HHS wide policies and

guidelines with regard to retention and destruction of individual information in identifiable form (IIF) will be followed.

Technical Controls include user identification, passwords, updated firewalls, encryption

Physical Controls in the production environment include guards, cipher locks, biometrics and closed circuit television. Physical Controls in the development environment include key cards, visitor logs,

Identify the publicly-available URL:

https://www.thinkculturalhealth.hhs.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.

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?

Yes

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

Yes