US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

05/22/2017

OPDIV:

FDA

Name:

CTP Retailer Education Community

PIA Unique Identifier:

P-1935428-488620

The subject of this PIA is which of the following?

Minor Application (child)

Identify the Enterprise Performance Lifecycle Phase of the system.

Implementation

Is this a FISMA-Reportable system?

No

Does the system include a Website or online application available to and for the use of the general public?

Yes

Identify the operator.

Agency

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.

The FDA Center for Tobacco Products (CTP) oversees the implementation of the Family Smoking Prevention and Tobacco Control Act. Some of the Agency's responsibilities under the law include setting performance standards, reviewing premarket applications for new and modified risk tobacco products, requiring new warning labels, and establishing and enforcing advertising and promotion restrictions.

The Family Smoking Prevention and Tobacco Control Act requires and permits communications to inform consumers and the general public about the risks of tobacco products. As such, public education campaigns that educate consumers about the risks of tobacco products contribute to carrying out the Act's purposes by disseminating health risk information and by helping ensure tobacco users and nonusers have a better understanding of the health risks.

The CTP Retailer Education Community (REC) is a website developed to answer the needs of professionals (referred to throughout this Privacy Impact Assessment as users) working to educate tobacco retailers around the United States about federal and local tobacco regulation. These professionals who are the primary users of REC can be both state/local government employees and educators from private organizations.

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

The CTP REC is a website moderated by CTP personnel (employees and direct contractors). It offers four main features:

Interactive Discussions: The website hosts a discussion board where users and moderators can initiate and participate in discussions about topics such as tobacco sale regulations, retailer education best practices, and other retailer education related issues of interest. Users create profiles visible to other users on the site to increase transparency among participants and build an authentic community.

Community Calendar: The website provides a moderated community calendar containing information about tobacco retailer education events happening around the United States.

State and Local Materials Library: The website includes a state and local materials library that features CTP-moderated (monitored and controlled) content including materials such as posters, flyers, and calendars used for tobacco retailer education submitted by the website users and vetted by the website moderators.

FDA Materials: The website provides CTP published tobacco retailer education campaign materials for download by website users.

The system collects and stores user submitted profile information, event information, state and local education materials, and online discussion content. The system also collects and stores user-submitted data to create their accounts including: first name, last name initial, organization name, state, city, county (optional), e-mail, and optional photograph. This information (with the exception of the e-mail address) is available to and shared among authorized users of the Website when they are logged in and using the services of the online community.

CTP employees and direct contractors access the system to perform administrator and moderator duties. They access the system via a single-sign-on process using multi-factor authentication. Public users must be approved in order to be granted access to REC. Once approved, they access the system using an assigned username and a temporary password provided to them via e-mail. Users can reset their temporary password to a password of their choosing that meets complexity standards.

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

The REC system is a digital information exchange and discussion platform for tobacco retailer education practitioners. The site is hosted in a domain under HHS.gov, but FDA operates and maintains it. Through the web site, FDA collects and maintains two general types of information: User profile information and user submitted content.

User profile information: REC collects and maintains user profile information submitted by users to develop a contact directory that will help users to build a community. This information is only shared with other validated (logged in) users. Each user has an individual ‘homepage’ that includes their submitted biographical information and indicates how other users can send them messages. Site moderators or administrators are also able to view this information as part of their work overseeing the community. Users and administrators may conduct site searches by state and organization type, but not by name or other PII. Records are not retrieved by personal identifier.

REC collects and maintains users' submitted content such as discussions and their replies, events, and state and local educational materials. The system also maintains geographic location data submitted for inclusion in user profiles. Location data is limited to city and state, and county if the user chooses to provide it. FDA uses this data to display the number of Tobacco Retailer compliance checks implemented by CTP Compliance Officers in each user's home state on the user's own personalized REC homepage.

User-submitted content: User-submitted content such as events and state and local materials are approved by moderators before the content is published on the web site. Users may ask the moderator of the site to edit or delete submitted information at any time. Information about events that have passed is eventually archived.

CTP moderates the site during the week (M-F) during business hours. Content added to the state and local materials and events pages is approved before posting. CTP moderators review discussions periodically through the day to ensure that they are on-topic, accurate, and appropriate for disclosure. CTP has also developed a response bank to help guide moderation of discussions.

FDA does not save any content that is submitted by a user and not approved by moderators for posting.

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

Yes

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

Name

Photographic Identifiers

E-Mail Address

Employment Status

City, state and county, username and associated password, HHS

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

Public Citizens

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

“Public Citizens” refers to professionals participating in the online engagement platform.

How many individuals' PII is in the system?

100-499

For what primary purpose is the PII used?

The primary purpose of using PII in the system is to build an authentic, interactive community that will support and enhance the work of tobacco retailer educators. The system includes profiles for users that include PII to achieve this goal.

Moderators and administrators use PII to validate accounts, to create user profiles, and to send users automatic notifications from the system addressing account requests and approvals, event submissions and approvals, or document submissions and approvals.

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

The secondary purpose of using geographical PII related to city, state and country is to determine the number of Tobacco Retailer compliance checks conducted in the users' home state.

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

Federal Food, Drug and Cosmetic Act (FFD&C) (21 U.S.C. Section 301 et seq., at 321(rr) and Chapter IX). See, e.g., Sections 2, 3, 105, 201, 204, 904, and 908.

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

No

Identify the sources of PII in the system.

Online

Government Sources

State/Local/Tribal

Non-Governmental Sources

Public

Private Sector

Identify the OMB information collection approval number and expiration date

Not applicable.

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.

Users self-submit their PII. They receive notice of the collection and use of their information in the following ways: (1) at the point of submitting their PII (completing an online form requesting permission to join REC) users must review and affirmatively accept terms and conditions; (2) REC provides a privacy notice and disclaimer and users can access HHS policies posted on HHS.gov; (3) REC users are informed of the data collection process prior to voluntarily submitting data to CTP; and (4) this Privacy Impact Assessment which will be made available to the public on the internet.

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.

All community membership is voluntary. Users who want to join the community are required to share the basic personally identifiable information needed to create their profile; the transparency provided by basic public profiles is critical to building the user-desired community. If users do not agree to submit their information, they can decline the REC terms and user agreement. In that case, REC will not proceed with creating a user account and will not store user information.

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

FDA does not expect to conduct major changes to the Website that would affect the privacy of community participants, or how individuals' information is collected or stored. Individuals whose PII is in the system will be notified of a major change by the most efficient and effective means available and appropriate to the specific change(s). This may include a formal process involving written and/or electronic notice, or informal processes such as email notice to the individuals.

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 may reach out directly to the FDA CTP REC moderators through the Website with any concerns about the use of their PII. Users can delete their own accounts and all of the content that they have provided to the community (except archived event information) without prior approval at any time. All of the user's account information is deleted after they delete their accounts, and the community information related to the user is moved to an anonymous account.

Additionally, individuals have the ability to notify and seek assistance from CTP using dedicated phone numbers and/or a dedicated email address. This information is available on FDA.gov.

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

Data integrity and accuracy are important to the extent that PII permits communication on the platform. Moderators review PII as it enters the system when they review sign-up forms submitted by individuals requesting an account. This review process ensures that no PII aside from first name and e-mail address are included in accounts when they are created.

Moderators also undertake periodic reviews of all photos submitted by users to ensure that they do not contain any unexpected PII (for example, in a text overlay).

Integrity, as well as availability, are both protected by security controls selected according to the risk level of the system and consistent with federal guidance from the Office of Management and Budget(OMB) and the National Institutes of Standards and Technology (NIST).

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

Users:

Users with approved accounts have access to viewing all other users' public profiles on the web site. They require this access to advance the purpose of the site as being a community network. Profiles help users get to know who they are interacting with and provide context for introductions.

Administrators:

Administrators and moderators have access to public profile information in the normal course of their work reviewing user submitted content and discussions.

Developers:

Developers have access to the data to test functionality and ensure code is working properly.

Contractors:

All developers are CTP direct contractors and need access to the data to test and ensure the code is working properly.

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

CTP employees and direct contractors with valid network accounts who require access to REC must have supervisory approval and signature before access is granted. Access is granted based on a business need. Users of the REC community request access through the sign up form on the website. The agency reviews the system access list on a quarterly basis to adjust access roles and permissions and delete unneeded accounts from the system.

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.

A Standard Operating Procedure (SOP) and System Access Request (SAR) form are used to grant different levels of system access based on work need and role. The relevant supervisor indicates on the REC user account creation form the minimum access that is required in order for the user to complete his/her job. The scope of access is restricted based on role-based criteria.

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.

FDA provides mandatory IT security and privacy awareness training for all FDA personnel. A portion of this training is dedicated to the protection of PII overall for the agency.

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

Moderators receive an operational handbook outlining their responsibilities for safeguarding PII and the procedures for review and approval of content.

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 data captured in REC will be retained indefinitely, pending receipt of an FDA file code consistent with the National Archives and Records Administration (NARA) guidelines. FDA will update this Privacy Impact Assessment with this information in the future.

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

Administrative safeguards include user training; system documentation that advises on proper use;

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

Administrative safeguards include user training; system documentation that advises on proper use; implementation of Need to Know and Minimum Necessary principles when awarding access, and others. Technical Safeguards include use of multi-factor access authentication, firewalls, and network monitoring and intrusion detection tools. Physical controls include that all system servers are located at facilities protected by guards, locked facility doors, and climate controls. Other appropriate controls have been selected from the National Institute of Standards and Technology's (NIST's) Special Publication 800-53, as determined using Federal Information Processing Standard (FIPS) 199.

Identify the publicly-available URL:

https://stage-retailered.betobaccofree.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?

No

Does the website have any information or pages directed at children under 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