US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

04/11/2022

OPDIV:

ACF

Name:

Title IV-E Prevention Services Clearinghouse

PIA Unique Identifier:
P-2481148-429763

The subject of this PIA is which of the following?
Major Application

Identify the Enterprise Performance Lifecycle Phase of the system.
Operations and Maintenance

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.
Contractor

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 Family First Prevention Services Act (FFPSA) of 2018, as codified in Title IV-E of the Social Security Act, authorized new optional funding for time-limited prevention services for mental health, substance abuse, in-home parent skill-based programs, as well as kinship navigator programs intended to support children and families and prevent foster care placement. In accordance with FFPSA, the Title IV-E Prevention Services Clearinghouse (PSC) established by the Administration for Children and Families (ACF) within the U.S. Department of Health and Human Services (HHS) to conduct an independent systematic review of research on these programs and services. State title IV-E agencies may claim reimbursement for programs and services. The Prevention Services Clearinghouse only contains reviews and ratings of prevention and treatments services. Some state agencies can ask Children’s Bureau to reimburse them for money spent on prevention and treatment services if those services are rated and reviewed on the PSC website by PSC and are identified in the state’s five-year title IV-E prevention program plan (see ACYF-CB-PI-18-09, ACYF-CB-PI-18-10, and ACYF-CB-18-11 for further details).

The Prevention Services Clearinghouse reviews publicly available child welfare studies to rate programs and services. This information does not contain personally identifiable information. The Prevention Services Clearinghouse website (https://preventionservices.abtsites.com) makes the program or service ratings available to stakeholders, including state title IV-E agencies. The website also allows stakeholders to access descriptions of programs and services; obtain detailed information about the review process and ratings; find answers to Frequently Asked Questions, including the working list of programs and services currently under review; and sign up for email updates.

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

PSC is used to develop the ratings for each program and service. PSC contains publicly available studies, study reviews, and related records (e.g., citations of the publicly available study). The study reviews have associated comparisons, outcomes, and contrasts, all of which are ultimately associated with a program record. When a program record is published, the data from all study reviews associated with the program, or service are evaluated to determine a rating for the program or service. This rating is reported on the website, along with information about the studies reviewed for that program or service.

PSC has a public-facing website containing program pages and a faceted search interface for those pages, along with other public website content (e.g., home page, FAQs, about page, review process pages). Individuals who visit the website can sign up for email updates on changes to the PSC website through MailChimp. (https://preventionservices.abtsites.com/subscribe).

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

The internal system is only available to contractors of ACF users who maintain and update the system. They provide their name and email address to acquire a user login and account. Once in the system, they enter various information extracted from publicly available journal articles (i.e., PII about service recipients and any other non-public information have already been removed).

The system is also available to the general public. Anyone can subscribe to the PSC by providing their email addresses; those who do will receive notifications when the website is updated. Along with their email address, it asks what position best describes them and their area of interest; their position and area of interest can be used to customize messaging for specific audiences. This information is managed by contractor staff through the MailChimp administrator interface and is not used for any other purpose.

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

Yes

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

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

How many individuals' PII is in the system?

500-4,999

For what primary purpose is the PII used?

For employees and the contractors, it’s to uniquely identify users of the system for system authentication.

For public citizens, it’s whomever provides their email address voluntarily to get notifications of updates to the site.

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

There are no secondary uses for the PII.

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

Social Security Act Title IV-E, as amended by the Bipartisan Budget Act of 2018

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

No

Identify the sources of PII in the system.

Identify the OMB information collection approval number and expiration date

Not applicable - OMB information collection approval number is not needed for PSC because this system does not have a form for OMB collection for public information.

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.

PSC’s users are notified via email that their personal will be collected and used for the purposes of creating an account in the system upon joining the team and final approval of government team leads.

For email subscribers, the signup form is embedded in a page with a notification that their information will only be used to send them emails with updates to the website. The email subscribers receive an email when the PSC website is updated.

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.

System users can object to the collection of their PII at the time of account creation, however this would result in the individual not being granted access to the system.

Public users can object to entering their email address, but then they will not receive the email updates.

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

The PSC team is notified via email or a message within the application when a major change is made to the system that would impact an individual’s PII

For public users, we would send them an email message via MailChimp. All email communications have a link that allows the reader to unsubscribe from the email notification system.

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 has a concern about their PII, they can contact the program team managers and leads.

The public website has an email link to the contract staff project mailbox for the public users. Public users could email us if they felt their email address had been compromised through our site.

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

For the system users:
Integrity: The system users are assigned a level of access based on their role. When the project began, either a high-level system administrator or manager reviewed each user's level of access to assure it was correct level. One of those two individuals assess whether each new user receives the correct level of access and remove each user who leaves the project. On an annual or more frequent basis, one of those individuals also reviews each user to make sure they continue to need the same level of access.
Availability: The site database is backed-up daily to allow easy restoration, and has historically been available 99.95% of the time.
Accuracy: When the project began, either a high-level system administrator or manager reviewed each user's level of access to assure it was correct level. On an annual or more frequent basis, one of those individuals reviews each user to make sure they continue to need the same level of access.
Relevancy: The system users are assigned a level of access based on their role. On an annual or more frequent basis, either a high-level system administrator or manager reviews each user to make sure they continue to need the same level of access.

For the public user emails, MailChimp offers multiple layers of security to protect the integrity, availability, accuracy, and relevancy of user data stored in their systems:
Integrity: MailChimp account passwords are hashed; the entire application is encrypted with Transport Layer Security (TLS); and logins have brute force protection. All databases are dedicated, and logically separated to prevent corruption and overlap.
Availability: MailChimp has mirrored account databases with regular off-site backup and an infrastructure continuity plan for their multiple, geographically dispersed, data centers.
Accuracy: Public users can opt out on their own if their information is inaccurate and can contact us to request that they be removed from the mailing list.
Relevancy: Public users can opt out on their own, but we do not contact them to see if they wish to continue to receive emails.

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

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

The Prevention Services Clearinghouse has a role-based access system with three types of users:
Regular System Users: The direct contractor staff who use the system to rate the Title IV-E Prevention Services can only see, at most, which other Regular System User was responsible for what part of the rating process (e.g., Reviewers can see the name of the assigned Reconciler for the

studies they're reviewing).
PSC Administrators: Some direct contractor staff who are responsible for managing the Prevention Services Clearinghouse can access the name and email of the other direct contractor staff who use the system; all receive access to the least amount of PII necessary for their role.
Public Users: Members of the public who visit the website cannot see any PII about anyone.

MailChimp also has a limited role-based access system:
MailChimp Users: Each member of the public who signs up to receive emails via MailChimp can see their own PII and manage their own account.
A small number of direct contractor staff have access to the name and email of each subscriber in order to view who is a subscriber and manage accounts.
Some MailChimp tech support and engineering staff also have access to those names and emails, but all MailChimp employees sign a Privacy Safeguard Agreement and undergo criminal history and credit background checks prior to employment.

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 entire system restricts access to PII using privileges assigned to their system account. If an individual is identified as an Administrator, then their system account will receive the appropriate privileges to perform account management duties.

For MailChimp, public users can access only their own account information. A small number of direct contractor System Administrators have access to all accounts in order to administer the listserv. MailChimp tech support and engineering staff can access the user data, but only access it if there is a tech support or other incident that would require accessing our user's data.

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.

PSC users receives HHS ACF security and awareness training at least annually and role-based security training to all personnel with significant information security roles a before granting access to the system, when changes are made, and at least annually per their policy.

All MailChimp employees are trained on best security practices, including how to identify social engineering, phishing scams, and hackers. They also sign a Privacy Safeguard Agreement outlining their responsibility in protecting PII.

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

All direct contract staff who enter data in the back-end system receive training on the standards and procedures of the systematic review and instructions on how to log in and record the findings from their study 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 Records Control Schedule (RCS) number for our Clearinghouses is: DAA-0292-2020-0005. Please be advised that this schedule is currently going through the approval process. For now, we treat the records as permanent.

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

The ability to change or create PII (name and email and contact information for users) is limited based upon least privilege and only granted to privileged users of the system.

Regarding the Prevention Services Clearinghouse:
Administrative Controls include requiring annual security awareness training to be completed by all users plus additional role-based security for privileged users of the system.
Technical Controls include positive user identification, passwords, least privilege access, and all the intrusion detection services provided by Amazon Web Services.
Physical Controls are inherited from the FedRAMP approved hosting platform, Amazon Web Services (AWS) GovCloud and include all the standard security controls for a commercial data center (security staff, visitor access procedures, intrusion detection system, fire suppression, uninterruptible power supply (UPS), climate controls, etc.)

Regarding MailChimp:
Administrative Controls include the requirement that all MailChimp employees complete a security training and sign a Privacy Safeguard Agreement outlining their responsibility in protecting PII.
Technical Controls include hashed passwords, encrypting the entire application, and an intrusion detection service.
Physical Controls include cameras, biometric scanners, and all standard data center controls.

Identify the publicly-available URL:

https://preventionservices.abtsites.com/

Note: web address is a hyperlink.

Does the website have a posted privacy notice?

No

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.

Other technologies that do not collect PII:

Google Analytics

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?

No