

US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

08/08/2024

OPDIV:

ACF

Name:

Home Visiting Evidence of Effectiveness Review

PIA Unique Identifier:

P-7377903-968100

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.

Agency

Is this a new or existing system?

Existing

Does the system have Security Authorization (SA)?

Yes

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

PIA Validation

No Changes to the information collected or stored in the application.

Describe the purpose of the system.

The purpose of the Home Visiting Evidence of Effectiveness (HomVEE) review website is to help the Department of Health and Human Services (DHHS) and the Administration for Children & Families (ACF) fulfill legislative requirements of the Maternal, Infant, and Early Childhood Home Visiting (MIECHV) Program. Legislation mandates grantees use the majority of grant funds to implement evidence-based home visiting models. Home visiting models are interventions or programs that deliver a specific set of activities in a family's home. Many home visiting models are designed to improve parent and child outcomes like health, school readiness, and parenting behaviors. Each model has its own set of standard components that are provided to families in order to improve these outcomes. HomVEE provides a catalogue of informational resources about these evidence-based home visiting program models targeting families with pregnant women and children from birth to kindergarten entry (up through age 5) to anonymous Internet users, including potential

grantees.

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

The HomVEE website displays information collected from a systematic review of research articles and papers as well as public websites about Home Visiting models. Specific data elements collected, maintained, and stored in HomVEE include:

1. Home visiting model program features: Model name, affiliated organization name, model components (e.g., curriculum name and description, number of home visits)
2. Research literature summary information: This includes information from each article or paper reviewed. Reviews include aggregate data on research design and study participants. Research design information includes research methods used in the study (e.g., Randomized Control Trial, Quasi-experimental Design) and outcomes tested in the study (e.g., maternal and child health, school readiness, parenting behaviors). Participant data includes the number of participants and demographic characteristics such as marital status, race, and income.
3. Study findings/conclusions (e.g., statistical significance)
4. Research citations including last name of author, first initial, publication date, and title
5. The system also contains information on the procedures and policies guiding the review of research.
6. Email addresses from public users that wish to receive website updates

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

The HomVEE project team conducts an annual broad Internet search for research articles and papers on home visiting models serving pregnant women or families with children from birth to age 5. In addition, they issue a call for studies (i.e., emails to listservs requesting authors submit their research articles). The team reviews and summarizes those articles to determine whether the home visiting models studies meet the DHHS criteria for an evidence-based model. The summaries created are reviewed for accuracy and then the selected documents are uploaded to the website by a system administrator. System administrators access and manage HomVEE through Drupal, a website content manager tool, hosted at ACF Office of Chief Information Office (OCIO) Amazon Web Services (AWS) General Support System (GSS) Their user credential are managed through this tool as well.

Public users voluntarily provide their email addresses in order to receive updates about the HomVEE website. These updates are sent about 3 times a year. Users opt in to these email updates and can opt out at anytime.

The HomVEE system uses the Drupal's module Simplenews to manage the email subscription on the HomVEE website. Once the user subscribes, the email address is added to the subscription list in the MySQL database. The user also has the option to unsubscribe at any time and the email will be removed from the subscription list. Users with HomVEE Drupal Administrator role will have permission to access through the HomVEE website to download the email subscription list.

To facilitate sending email updates to subscribers, the contractor stores temporary email addresses downloaded from HomVEE website in an access controlled, segregated HomVEE folder on the contractor's private network. Only approved HomVEE project staff can access the email list. Currently, Simplenews Drupal module is not being used to send emails regarding updates or other communication with subscribers.

The contractor downloads the email subscription list for multiple reasons. First, they download the list because they need to make sure that they have retained the latest subscriber list whenever they do website updates that would also overwrite the production database. Second, the email communication to the subscribers include emails addressed provided by the program office and were not subscribed through the website. They need to send the same message to some addresses

that are not “subscribed” because that is how they contact electronic mailing lists that HHS has designated as relevant to HomVEE communications. Finally, they have more control of the presentation of the email and how the email is sent so that it doesn’t get blocked as spam or junk email.

A proposed permanent records disposition is pending approval with the National Administration Records Archive (NARA). The disposition number is DAA-0292-2019-001. The proposed disposition states that all HomVEE records including PII (email addresses) will be maintained at ACF for 15 years then transferred to NARA after the cutoff (end of the calendar year).

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

User Credentials

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

Public Citizens

How many individuals' PII is in the system?

500-4,999

For what primary purpose is the PII used?

The primary use of PII in this system is to notify the user of any content updates to the HomVEE website.

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

There are no secondary uses

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

5 USC 301, Departmental regulations.

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

No

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

Online

Identify the OMB information collection approval number and expiration date

Electronic subscriptions to agency notifications or publications are excluded from the definition of "information" under PRA regulations. Thus, OMB collection approval does not apply to the email addresses collected for the HomVEE mailing list.

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 voluntarily provide their email addresses when they sign-up for the HomVEE mailing list. When they sign up they see the following notification: "Your information will not be shared with any third-party vendors or other government agencies and will be used only for HomVEE alerts."

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.

To opt-out users may select the "unsubscribe link", located in each email message that subscribers receive. Upon selecting "unsubscribe" the user email address is automatically deleted from the system.

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

The fundamental purpose of the website does not change, only the content is updated a few times a year. If for some reason the fundamental purpose of the website changes, we will delete all the email addresses collected and users will need to opt in again to receive the email notifications. Any new uses of PII or major changes will be indicated to users if they choose to "opt in" to the email notifications again.

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.

The HomVEE website has a link to the ACF privacy statement at the bottom of the webpage.

The "contact us" page (<https://homvee.acf.hhs.gov/help>) on the website has an email address (HomVEE@acf.hhs.gov) that users can contact as questions arise. Specifically, the page directs users to send HomVEE an email, if they have privacy concerns. If, ACF receives such a message to the ACF HomVEE mailbox, they will forward that concern to the contractor for investigation, and the contractor will research the matter and provide a prompt update on the findings.

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

Integrity: Prior to each email blast, the contractor will export the mailing list from the database and store the email list on the contractor's project folder on a secure internal network drive. The contractor will delete the email list from the project folder once the email blast has been completed. Access to email addresses is limited to users with access to a Drupal database. HomVEE Staff review Drupal account logs every 6 months to confirm operational need for the access. Those that are not necessary are disabled. The HomVEE Management team will notify the HomVEE Administrator when users no longer require access to the system or the need-to-know status changes. The HomVEE project manager annually reviews the access permission list to the contractors' internal network drive folder for HomVEE. Access to the internal network drive is managed by the contractors' Active Directory and approved by the project director. The contractor immediately reviews authorizations for information systems and facilities access and initiates appropriate actions. Such action may include revoking access privileges to the HomVEE system.

Availability: The AWS Backup and Recovery process will be performed and managed by the OCIO Operations Team. Full back-up snapshots of the AWS server volumes are taken daily at 12:00am EST. Notifications alert the Database Administrator in the event of a failed back-up and remediation options are provided to the Database Administrator. If the system goes down it is restored within 72 hours.

Accuracy: Any accuracy concerns can be emailed via the website to the HomVEE mailbox. The

accuracy of email addresses is periodically checked to eliminate any undeliverable email addresses. These "bounce back" email addresses are deleted from the database.

Relevancy:

Individuals with PII in HomVEE have the ability to update their email address by opting out and opting back in with their new email address. Additionally, PII records are maintained in accordance with NARA.

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 contractor provides access on a need to know and least privilege basis. Specifically, Administrators have site administrative role privileges to retrieve the email addresses from the Drupal site. Only Drupal users with the appropriate permission can access the MySQL database for email addresses. Those who have access to the email addresses on the contractor's project folder include project leadership and communications staff who are essential to communicating through those email addresses. All users are approved by the system owner before receiving access to 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.

PII access is limited select administrators, project leadership, and communications staff that are essential to communicating to HomVEE subscribers.

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.

As dictated in the contract between OPRE and the selected contractor managing HomVEE, the contractor must ensure that all of its employees, subcontractors (at all tiers), and employees of each subcontractor, who perform work under this contract/subcontract, are trained on data privacy issues and comply with the above requirements. The Contractor shall also submit a written plan and assurance for complying with the above requirements at least annually.

To fulfill this requirement, all contractor staff are required to complete annual security awareness training that covers, among other aspects, recognizing and safeguarding PII. The contractor provides basic security awareness training to all information system users (including managers, senior executives, and contractors) before authorizing access to the system, when required by system changes, and at least annually thereafter. At the start of employment, all contractor staff sign a confidentiality pledge and complete online security awareness training. Staff receive annual refresher training thereafter.

ACF staff users of HomVEE are required to annually complete Computer Security Awareness Training and review and sign the HHS rules of behavior.

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

The contractor's staff who work on the system receive ongoing training on content management in Drupal and the HomVEE review process.

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.

A proposed permanent records disposition is pending approval with the National Administration Records Archive (NARA). The disposition number is DAA-0292-2019-001. The proposed disposition states that all HomVEE records including PII (email addresses) will be maintained at ACF for 15 years then transferred to NARA after the cutoff (end of the calendar year).

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

HomVEE is hosted at ACF OCIO AWS GSS. The GSS has a shared responsibility model for the administrative, technical, and physical safeguards. Part of the responsibility lies with the operator, AWS, and the other part is implemented and managed by the OCIO infrastructure team. The physical controls are provided by AWS and include fire detection and suppression requirement, uninterruptible power supply (UPS) units, climate control, preventative maintenance, video surveillance and security staff, and a thorough access control policy.

When email addresses exported, the HomVEE project leverages the security capabilities of the contractor's secure on-premises applications and tools and the policies and procedures that have been implemented for the contractor's enterprise and specifically for the HomVEE project.

The technical controls are shared responsibility and include a fault-tolerant design to support high availability, network access control lists (NACLs), security groups, and route tables. The administrative controls managed by ACF include processes and procedures for account and change management, training requirements, and role-based access control (RBAC).

Administrative controls include policies and procedures around protection of PII including personnel screening, security awareness training, system procurement, separation of duties and least privilege, security planning, change control, auditing and periodicity of security assessments and reviews. Additionally, HomVEE only collects the minimum PII (email address) necessary to conduct the HomVEE project.

Technical controls include the numerous automated capabilities that enforce: access permissions to PII, encryption of PII in transit and at rest, password and multi-factor authentication requirements, audit logging/monitoring/alerting, network intrusion and prevention, and protection against malware.

Physical controls include facility security procedures such as protecting against unauthorized access to, loss of, and theft of PII, as well as procedures to protect the people who work on HomVEE project.

Identify the publicly-available URL:

<https://homvee.acf.hhs.gov/Default.aspx>

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.

Other technologies that do not collect PII:

Google Analytics

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?

No

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

null