US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

04/10/2026

OPDIV:

NIH

Name:

OD Mailchimp

PIA Unique Identifier:

P-6176798-070172

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?

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 Office of the Director (OD) Mailchimp is a cloud-based software service that provides a service for distributing informational communications, such as newsletters and announcements, to a voluntary external audience. The system's core function is to allow authorized internal staff to manage the complete life-cycle of email-based outreach, from collecting subscriber contact information to creating and sending content to a user base of public stakeholders who have opted-in to receive information. The system processes, stores, and transmits subscriber-provided email addresses.

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

The only personally identifiable information (PII) that the system processes, stores, and transmits are subscriber-provided email addresses and login information for Office of Behavioral and Social Sciences Research (OBSSR) system administrators (email and password).

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

The Office of the Director (OD) Mailchimp is a cloud-based software service that provides a service for distributing informational communications, such as newsletters and announcements, to a voluntary external audience. The system's core function is to allow authorized internal staff to manage the complete life-ycle of email-based outreach, from collecting subscriber contact information to creating and sending content to a user base of public stakeholders who have opted-in to receive information. The system processes, stores, and transmits subscriber-provided email addresses.

The only personally identifiable information (PII) that the system processes, stores, and transmits are subscriber-provided email addresses and login information for Office of Behavioral and Social Sciences Research (OBSSR) system administrators (email and password).

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

Yes

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

E-Mail Address
password

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

Public Citizens

How many individuals' PII is in the system?

5,000-9,999

For what primary purpose is the PII used?

The system's core function is to allow authorized internal staff to manage the complete life-cycle of email-based outreach, from collecting subscriber contact information to creating and sending content to a user base of public stakeholders who have opted-in to receive information.

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

NA

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

5 U.S. Code §301 and 302

42 U.S. Code § 241

42 U.S. Code § 282

42 U.S. Code § 284

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

In-Person

Non-Governmental Sources

Identify the OMB information collection approval number and expiration date

Public

NA. OD MailChimp does not solicit information from the public. Submission of an individual's email address is voluntary and not required by the program. Its only function is to allow individuals to sign up for newsletter communications.

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.

Submission of email addresses is voluntary and requires users to intentionally provide the contact information.

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.

Email communications include an option for the recipient to unsubscribe.

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

Individuals are notified via email.

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.

No process exists; individuals provide their email addresses voluntarily and that is the only PII within the 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.

Information collected is not modified after received.

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.

Only OBSSR administrators of the system, who manage the communication campaigns for the OBSSR, have access to the Mailchimp 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.

Determinations are made based on role-based access controls and least privilege. User rights are provisioned based on controls within the system, allowing users only access to the minimum amount of PII necessary to perform their job.

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.

According to NIH policy, all personnel who manage or operate NIH applications must successfully complete annual security awareness training. Training is completed on the http://irtsectraining.nih.gov site with valid NIH credentials.

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

NA

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.

11-502, Customer/Client Records. Delete when superseded, obsolete, or when customer requests the agency to remove the records (DAA-GRS-2017-0002-0002).

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

Administrative: Access is based on least privilege and is granted by the OBSSR system administrator.

Technical: The use of multi factor authentication to limit access to the system. As well as distributed denial-of-service mitigation software, data loss prevention and network scans, and data encryption at rest and in transit.

Physical: The system is hosted and ran by MailChimp. MailChimp uses biometric scanners for server access. Servers are guarded 24/7.

Identify the publicly-available URL:

https://nih.us18.list-manage.com/subscribe?u=90101cfda8ab653679a4df12c&id=fc23191f7f

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 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