US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

08/16/2016

OPDIV:

FDA

Name:

SendSuite Live

PIA Unique Identifier:

P-2027630-309613

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?

No

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.

SendSuite Live is a Commercial Off The Shelf (COTS) software application that FDA uses to provide a single solution for sending mail and streamlining the mailing process.

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

For FDA's use of SendSuite Live, the application will handle, and store mail and delivery service labeling associated with FDA's use of United Parcel Service (UPS) and United States Postal Service (USPS) delivery services. The application will also store tracking information and system user authentication information. The type of information that SendSuite Live collects, maintains and shares are the names, addresses and phone numbers for members of the public who receive mail from the FDA's mail operations.

The system will also hold the FDA office mailing address for agency offices sending mail and in some cases the name of individual employees sending outbound mail. FDA users employ system-specific access authentication/logon information to access SendSuite and this data is maintained within SendSuite.

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

SendSuite Live helps to facilitate FDA's mail operations by increasing the efficiency of the mailing process such as printing compliant labels and stamps to be placed on parcels being sent via US Mail or UPS. The information used and stored in the application includes United States Postal Service (USPS) and United Parcel Service (UPS) Tracking Number, USPS/UPS service type (e.g., First Class Mail, Priority Mail, etc.), USPS/UPS service type add-on information (e.g., Registered Mail, Certified Mail, etc.), mail recipient (addressee) name, mail recipient mailing street address and zip code, and value of postage used to send a parcel.

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

Yes

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

Name

Mailing Address

Phone Numbers

FDA personnel (user) logon information (Username and Password)

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

Employees

Public Citizens

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

Vendor/Suppliers/Contractors

Public citizens may include points of contact at regulated entities.

How many individuals' PII is in the system?

10,000-49,999

For what primary purpose is the PII used?

The PII is used to comply with UPS, USPS regulations for successfully sending parcels via US Mail in accordance with General Services Administration (GSA) Schedule 48 and GSA Domestic Delivery Services (DDS3) Blanket Purchase Agreement (BPA) Pricing.

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

Application data may be used for testing or training in a secure test environment. Zip codes of mailing recipients may be used for determining and forecasting postage expenses.

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

FDA's use of information in SendSuite is authorized by 5 U.S.C. 301 which permits agency heads to create the usual and expected infrastructure necessary for the organization to accomplish its purposes and mission. In addition, the security and privacy measures for the system are required by the Federal Information Security Management Act (FISMA) and the statutes underlying OMB Circular A-130 for the secure and efficient use of government systems and resources.

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

Hardcopy

Government Sources

Within OpDiv

Non-Governmental Sources

Public

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.

No prior notice. Name and mailing address are well established publicly accepted standard PII elements needed to send parcels via US mail with USPS/UPS. Members of the public are aware of and voluntarily provide their name and address when corresponding with FDA.

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.

If the recipient would like to request to opt-out of receiving mail from FDA, they may notify the FDA sender via mail or contact number to not send them mail via US Mail or UPS.

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

No such major changes are anticipated. The system only collects PII in accordance with UPS and USPS regulations. FDA relies on UPS and USPS to adequately communicate any changes in their regulations to the public.

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 individual should contact the US Postal Inspector Service, a federal agency with police powers whose sole mission is to investigate crimes or inappropriate use of information that involves USPS and/or USPS services. Individuals may contact FDA using contact information available on FDA.gov and by phone.

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

There is currently no process in place due to short duration of handling information. Current records control schedules have such data being destroyed after 1 year (and sometimes less) in most situations.

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

Users:

To send the mail parcel to clients.

Administrators:

To print reports for project manager and business owner as well as resolve account issues.

Developers:

Developers resolve major system issues.

Contractors:

Acting as administrators and/or users.

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

The Project Manager and Business System Owner review all user account requests, which contain justification, and utilize their subject matter expertise to determine if a true "need to know" exists before granting access.

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.

SendSuite Live only has the minimum amount of information necessary in order to mail documents which are the name, mailing address, and phone number for recipients. All system users need access to the PII involved in printing USPS compliant postage labels and stamps.

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.

All personnel take the mandatory yearly Information Security Awareness and Records Management Training. In addition, administrators with privileged accounts are required to take role-based training yearly to maintain account access.

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

The vendor for SendSuite provides system training for proper use of the system. FDA personnel may take advantage of information security and privacy awareness events and workshops held within FDA. Privacy guidance is also available via the FDA's privacy office.

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.

Logon credentials remain available as long as each user has authorized access to the system. Credentials are revoked when access is no longer needed, including if the individual moves to a different office within FDA or leaves FDA employment. These records are maintained under FDA File Code 9962 (NARA GRS 20, Item 1c; superseded by the new GRS 3.2, item 030 (DAA-GRS-2013-0006-0003), which is for “records … created as part of the user identification and authorization process to gain access to systems. " Under this schedule, retention is until "business use ceases." In other words, NARA concurs that agencies may dispose of these records as soon as they are no longer needed.

Other PII in the system: FDA Administrative Records Control Schedules-Administrative Management. File Code 9164, NARA Approved Citation GRS 23-8. Disposition: TEMPORARY. Destroy or delete when 2 years old, or 2 years after the date of the latest entry, whichever is applicable.

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 role-based access settings, firewalls, passwords and others. Physical controls include that all system servers are located at FDA 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. Technical settings ensure that only Administrators are allowed to reset the password for users if needed. If a user that is not given access to the Active Directory group attempts to access the link, the application will open but they will not be able to log into it.