



7710-12

## **POSTAL SERVICE**

### **Privacy Act of 1974; System of Records**

**AGENCY:** Postal Service™.

**ACTION:** Notice of new system of records.

**SUMMARY:** The United States Postal Service® (Postal Service) is establishing a new General Privacy Act System of Records. This new system of records is being established to provide administrative support to end users in connection with a new Postal Service digital application, USPS Health Connect™.

**DATES:** This system will become effective without further notice on [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER] unless, in response to comments received on or before that date, the Postal Service makes any substantial change to the purpose or routine uses set forth, or to expand the availability of information in this system, as described in this notice.

**ADDRESSES:** Comments may be mailed or delivered to the Privacy and Records Office, United States Postal Service, 475 L'Enfant Plaza SW, Room 9431, Washington, DC 20260-1101. Copies of all written comments will be available at this address for public inspection and photocopying between 8 a.m. and 4 p.m., Monday through Friday.

**FOR FURTHER INFORMATION CONTACT:** Matthew J. Connolly, Chief Privacy Officer, Privacy and Records Office, 202-268-8582 or *privacy@usps.gov*.

**SUPPLEMENTARY INFORMATION:** This notice is in accordance with the Privacy Act requirement that agencies publish their amended systems of records in the *Federal Register* when there is a revision, change, or addition.

### **I. Background**

The Postal Service seeks to provide a new wellness benefit to its employees and their dependents by offering USPS Health Connect, a secure application that allows end users to collect, store, and manage their personal health and wellness information in an account completely under the end user's control. Postal Service employees will be able to voluntarily elect to use this application.

### **II. Rationale for Changes to USPS Privacy Act Systems of Records**

The System of Records USPS 100.450, Administrative Records Related to Digital Services, is being established to provide administrative support to assist end users with technical questions and issues concerning the USPS Health Connect application. This new system of records includes only the categories of administrative records defined below. Neither the Postal Service nor its contractors or subcontractors will view or access any health or medical information that is collected, stored, or shared by the end user when using USPS Health Connect.

### **III. Description of New System of Records**

The Postal Service™ is establishing a new General Privacy Act System of Records titled: 100.450 Administrative Records Related to Digital Services. Pursuant to 5 U.S.C. 552a (e)(11), interested persons are invited to submit written data, views, or arguments on this proposal. A report of the new system of records has been sent to Congress and to the Office of Management and Budget for their evaluation. The Postal Service does not expect this notice to have any adverse effect on individual privacy rights.

Accordingly, for the reasons stated above, the Postal Service proposes a new system of records as follows:

**USPS 100.450**

**SYSTEM NAME:**

User Profile Support Records Related to Digital Service.

**System Location**

Contractor sites.

**Categories of Individuals Covered by the System**

1. Current and former USPS employees and their dependents that voluntarily opt-in to use USPS Health Connect.

**Categories of Records in the System**

1. *User Profile Information:* Name, date of birth, email, gender, phone, internally assigned identifier, username, physical address, employee identification number (EIN), contact information, customer ID(s), text message number, date of account creation, method of referral to website, date of last logon, and authentication method preferences.

2. *User preferences for communications:* Frequency and channel opt in/opt out and preferred means of contact for service alerts and notifications, language.
3. *Online user information:* Internet Protocol (IP) address, domain name, operating system versions, browser version, date and time of first and last connection, and geographic location.
4. *Identity verification information:* username, user ID, email address, text message number, and results of identity proofing validation.

#### **Authority for Maintenance of the System**

39 U.S.C. 1003, 1004, and 1201-1209.

#### **Purpose(s)**

1. To provide administrative support to assist end users with technical questions and issues.
2. To provide account management assistance.
3. To provide account security and to deter and detect fraud.

#### **Routine Uses of Records Maintained in the System, Including Categories of Users and the Purposes of Such Uses**

Standard routine uses 1-9 and 11 apply.

#### **Policies and Practices for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System**

##### ***Storage***

Automated database, computer storage media, and digital files.

##### ***Retrievability***

For System administrators and/or customer service representatives, by internally assigned identifier, or end user account details such as name, phone number, etc. to assist end users with access/use of USPS Health Connect and understand and fulfill end user needs.

### ***Safeguards***

Contractor site utilizes a Cloud Infrastructure under Agency Authorization to Operate (ATO) using a FedRAMP accredited Third Party Assessment Organization (3PAO) for selected Cloud Service Provider services.

Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. All physical access to data centers by contractor employees is logged and audited routinely.

Encryption and Data Security uses Federal Information Processing Standards (FIPS) compliant encryption, secure certificates for Client and Server communication authenticity, session protection certificates for end to end protection, multiple layers of protection for data confidentiality and integrity and hashes and password storage encryption and block level encryption for the data volumes. Customer support personnel have minimum access to user profile records.

### ***Retention and Disposal***

Records are retained until (1) the end user cancels the account, (2) six years after the end user last accesses their account, (3) until the relationship ends, or (4) after reasonable notice has been provided to the end user to export their account information in the event the agreement is terminated.

Records existing on computer storage media are destroyed according to the applicable USPS media sanitization practice.

### **System Manager(s) and Address**

Chief Information Officer and Executive Vice President, United States Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260.

### **Notification Procedure**

Individuals wanting to know if information about them is maintained in this system must address inquiries in writing to the system manager. Inquiries must include full name, Date of Birth, physical address, email address, username and other identifying information if requested.

### **Record Access Procedures**

Requests for access must be made in accordance with the Notification Procedure above and USPS Privacy Act regulations regarding access to records and verification of identity under 39 CFR 266.6.

### **Contesting Record Procedures**

See Notification Procedure and Record Access Procedures above.

### **Record Source Categories**

Individual end user.

\* \* \* \* \*

**Stanley F. Mires,**

*Attorney, Federal Compliance.*

[FR Doc. 2015-20031 Filed: 8/13/2015 08:45 am; Publication Date: 8/14/2015]