Save

Privacy Impact Assessment Form

v 1.47.4

Status: Draft | Form Number: F-68239 | Form Date: 4/13/2020 9:16:22 AM

	Question	Answer
1	OPDIV:	CDC
2	PIA Unique Identifier:	P-7011560-917071
2a	Name:	Amyotrophic Lateral Sclerosis Web Portal (ALS)
3	The subject of this PIA is which of the following?	○ General Support System (GSS) ○ Major Application ○ Minor Application (stand-alone) ◉ Minor Application (child) ○ Electronic Information Collection ○ Unknown
3a	Identify the Enterprise Performance Lifecycle Phase of the system.	Operations and Maintenance
3b	Is this a FISMA-Reportable system?	○ Yes ◉ No
4	Does the system include a Website or online application available to and for the use of the general public?	◉ Yes ○ No
5	Identify the operator.	◉ Agency ○ Contractor
6	Point of Contact (POC):	POC Title: Medical Epidemiologist POC Name: Paul Mehta POC Organization: ATSDR POC Email: pum4@cdc.gov POC Phone: 770-488-0556
7	Is this a new or existing system?	◉ New ○ Existing
8	Does the system have Security Authorization (SA)?	○ Yes ◉ No
8b	Planned Date of Security Authorization	June 18, 2020 ☐ Not Applicable

Save

11	Describe the purpose of the system.	The purpose of the Amyotrophic Lateral Sclerosis (ALS) Web Portal is to obtain more complete information on the likely prevalence of ALS ("Lou Gehrig's Disease"), and to better describe the demographic characteristics (age, race, sex, and geographic location) of those with ALS. The secondary goal of the surveillance system is to collect additional information on potential risk factors for ALS including, but not limited to, family history of ALS, smoking history, and military service. These risk factors were chosen because they are the only known and consistently recognized risk factors for ALS, and we want to obtain baseline assessment of basic risk factors on the registry participants. This information could then be used to design studies about what causes ALS.
12	Describe the type of information the system will collect, maintain (store), or share. (Subsequent questions will identify if this information is PII and ask about the specific data elements.)	The ALS Web Portal will collect, maintain, or share the following types of information: Patient Registration (Name, Race, Gender, Date of Birth [month/year], Email, City, State, Country, Social Security Number [SSN]) Security Questions (First Car, Favorite Color, First Pet Name, etc.) Patient Surveys (Military Status, Health Notes, Employment, Demographics, Work history, Alcohol & Smoking Consumption, Family History, etc.) Information Requests (Name, Address, Email, Phone Number). During patient registration, SSN [last 5 digits] and date of birth are only stored in the system temporarily and moved to another server daily. ALS Patients cannot retrieve or view their SSN after it is collected. ALS authenticates external (public) users with username (user's email address) and password which are stored in the system. Internal users are authenticated via CDC's Active Directory (AD). AD is a separate system with its own PIA.

Save

13	Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.	The purpose of the ALS Web Portal is to provide users with more information regarding the disease and to facilitate research for medical professionals and individual researchers. Researchers may request de-identified survey data for their own research. Identifiable data is shared with external researchers. The system collects registration information, surveys, and security questions from users of the site. These users are members of the public with ALS and are over 18 years of age. Registration information is used to uniquely identify participating individuals in the registry, for account support, and to contact the patients. Security questions are used if the patients forget their passwords. Surveys data is used to identify risk factors for ALS and inform research looking into the cause(s) of ALS. Patient Registration (Name, Race, Gender, Date of Birth [month/year], Email, City, State, Country, Social Security Number [SSN]) Security Questions (First Car, Favorite Color, First Pet Name, etc.) Patient Surveys (Military Status, Health Notes, Employment, Demographics, Work history, Alcohol & Smoking Consumption, Family History, etc.) Information Requests (Name, Address, Email, Phone Number) are collected. The system collects information request data in order to mail brochures. This data is collected from members of the general public and is not directed at children. Data is regularly retrieved from the system using ALS patient name, email address, or phone number for account maintenance or user verification. SSN is also used to match with data in other systems so that ALS patients are not double counted. ALS authenticates external (public) users with username and password which are stored in the system. The username is the user's email address. Internal user are authenticated via CDC's Active Directory (AD) AD is a separate system covered by its own PIA.
14	Does the system collect, maintain, use or share **PII**?	(•) Yes ( ) No

Save

15	Indicate the type of PII that the system will collect or maintain.	☒ Social Security Number ☒ Date of Birth ☒ Name ☐ Photographic Identifiers ☐ Driver's License Number ☐ Biometric Identifiers ☐ Mother's Maiden Name ☐ Vehicle Identifiers ☒ E-Mail Address ☒ Mailing Address ☒ Phone Numbers ☐ Medical Records Number ☒ Medical Notes ☐ Financial Account Info ☐ Certificates ☐ Legal Documents ☐ Education Records ☐ Device Identifiers ☒ Military Status ☒ Employment Status ☐ Foreign Activities ☐ Passport Number ☐ Taxpayer ID Gender Responses to security questions User credentials (user name and password)
16	Indicate the categories of individuals about whom PII is collected, maintained or shared.	☐ Employees ☒ Public Citizens ☐ Business Partners/Contacts (Federal, state, local agencies) ☐ Vendors/Suppliers/Contractors ☒ Patients Other
17	How many individuals' PII is in the system?	10,000-49,999
18	For what primary purpose is the PII used?	The PII is used to facilitate research for medical professionals and individual researchers.
19	Describe the secondary uses for which the PII will be used (e.g. testing, training or research)	The SSN is used as a quality check to prevent the submission of duplicate records.
20	Describe the function of the SSN.	The Registry is only asking for the last 5 digits of the Social Security number, not the entire 9 digit number. Because the Registry identifies cases of ALS from multiple sources, including from Medicare and the Veterans Administration, the Registry needs to make sure people are not counted twice. The only way to be sure that two people with the same or similar names are not the same person is with a partial Social Security number.
20a	Cite the **legal authority** to use the SSN.	E.O. 9397, as amended by E.O. 13478.
21	Identify **legal authorities** governing information use and disclosure specific to the system and program.	ALS Registry Act, Public Law No: 110-373

Save

22	Are records on the system retrieved by one or more PII data elements?		(•) Yes ( ) No
22a	Identify the number and title of the Privacy Act System of Records Notice (SORN) that is being used to cover the system or identify if a SORN is being developed.	Published:	09-19-0001, Records of Persons Exposed or Potentially Exposed to Toxic or Hazardous Substances
		Published:	
		Published:	
			☐ In Progress
23	Identify the sources of PII in the system.		Directly from an individual about whom the information pertains ☐ In-Person ☐ Hard Copy: Mail/Fax ☐ Email ☒ Online ☐ Other Government Sources ☐ Within the OPDIV ☐ Other HHS OPDIV ☐ State/Local/Tribal ☐ Foreign ☐ Other Federal Entities ☐ Other Non-Government Sources ☒ Members of the Public ☐ Commercial Data Broker ☐ Public Media/Internet ☐ Private Sector ☐ Other
23a	Identify the OMB information collection approval number and expiration date.		OMB 0923-0041, 01/31/2023
24	Is the PII shared with other organizations?		( ) Yes (•) No
25	Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason.		Individuals are notified during the self-registration process before creating an account, how their data will be used in the ALS System via a Privacy Notice screen.
26	Is the submission of PII by individuals voluntary or mandatory?		(•) Voluntary ( ) Mandatory
27	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.		There is a customized Consent Form that allows ALS patients to agree or disagree with CDC/ATSDR's terms. The decision of the patient is voluntary and will determine whether or not an account is created.

Save

28	Describe the process to notify and obtain consent from the individuals whose PII is in the system when major changes occur to the system (e.g., disclosure and/or data uses have changed since the notice at the time of original collection). Alternatively, describe why they cannot be notified or have their consent obtained.	In the event of significant system changes, a modified SORN would be published in the Federal Register. Further, the current PIA would be modified and published addressing the changes and identifying any new, resulting privacy considerations.
29	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 no process exists, explain why not.	Users can contact ATSDR via the contact information provided on the ALS website if any issues occur. Individuals should reasonably identify the record and specify the information being contested, the corrective action sought, and the reasons for requesting the correction, along with supporting information to show how the record is inaccurate, incomplete, untimely, or irrelevant.
30	Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy. If no processes are in place, explain why not.	The data is downloaded and cleaned annually. It is reviewed for accuracy – duplicates are removed, all fields are reviewed for relevancy and consistency. Statisticians check all data against these requirements and a "clean" file is produced. This file then is provided to and independent Statistician for validation. If any discrepancies are found the data is reviewed manually and any discrepancies are resolved. If changes or updates to the database is required those changes are completed based on the validation process. This cleaned and validated file is now the official file.
31	Identify who will have access to the PII in the system and the reason why they require access.	☐ Users: ☒ Administrators: Administrators need access to maintain data. ☐ Developers: ☐ Contractors: ☒ Others: Statisticians need access to analyze data.
32	Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Role-based access procedures are used to determine who will have access to PII in the system.
33	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 least privilege method is used to ensure that those with access to PII are only able to access the minimum amount necessary to perform their job responsibilities. Examples of controls that are employed are: (1) SQL read/write permissions that are controlled by user roles and privileges. (2) Active Directory controls administrator access. (3) E-Authentication control for external users.
34	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.	Personnel are required to undergo Annual Security and Privacy Awareness Training (SAT).

Save

35	Describe training system users receive (above and beyond general security and privacy awareness training).	None
36	Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices?	(•) Yes ( ) No
37	Describe the process and guidelines in place with regard to the retention and destruction of PII. Cite specific records retention schedules.	Records are retained, disposed, stored, handled, and viewed in accordance with the ATSDR Comprehensive Records Control Schedule (B-371), GSR 20.2c& d, and GSR 20.6. Current procedures allow the system manager to keep the records for 20 years unless needed for further study. Registry records will be actively maintained as long as funding is provided for by law. Retention periods vary depending on the type of record. Source documents for computer tapes or disks are securely disposed of when no longer needed in the study as determined by the system manager, and as provided in the signed consent form, as appropriate.
38	Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.	Administrative: Users are assigned unique roles and privileges depending on their user status. ALS patients are able to create an "ALS Patient" account, while all other public users are required to create a "Public" account. The ALS "System Administrator" can manage patient and public accounts and download data. ALS Patients must also pass a validation process before creating an ALS Patient Account. The validation process is a series of questions that determine if a patient has ALS. The general public can create a Public account without going through a validation process. Technical: PII fields will be masked on the GUI depending on the sensitivity of the data. For example the last 5 numbers of the SSN will be masked. All PII including SSN will be encrypted using CDC approved methods. To encrypt/decrypt data in database columns designed to hold PII data, a user must be given access to open and close a symmetric key. Physical Controls: Production and test servers are stored in a server room secured by the CDC. Access tools are in place to secure entry into CDC buildings (Guards, ID Badges, Key Card, Cipher Locks, and Closed Circuit TV).
39	Identify the publicly-available URL:	http://wwwn.cdc.gov/als
40	Does the website have a posted privacy notice?	(•) Yes ( ) No
40a	Is the privacy policy available in a machine-readable format?	(•) Yes ( ) No
41	Does the website use web measurement and customization technology?	(•) Yes ( ) No

Save

		Technologies	Collects PII?
41a	Select the type of website measurement and customization technologies is in use and if it is used to collect PII. (Select all that apply)	☐ Web beacons	○ Yes ○ No
		☐ Web bugs	○ Yes ○ No
		☒ Session Cookies	○ Yes ◉ No
		☐ Persistent Cookies	○ Yes ○ No
		Other...	○ Yes ○ No
42	Does the website have any information or pages directed at children under the age of thirteen?		○ Yes ◉ No
43	Does the website contain links to non- federal government websites external to HHS?		○ Yes ◉ No
	General Comments		
	OPDIV Senior Official for Privacy Signature	Beverly E. Walker -S Digitally signed by Beverly E. Walker -S Date: 2020.06.16 14:46:16 -04'00'	