Attachment 11
Privacy Impact Assessment

PIA SUMMARY

1

The following required questions with an asterisk (*) represent the information necessary to complete the PIA Summary for transmission to the Office of Management and Budget (OMB) and public posting in accordance with OMB Memorandum (M) 03-22.
Note: If a question or its response is not applicable, please answer “N/A” to that question where possible. If the system hosts a website, the Website Hosting Practices section is required to be completed regardless of the presence of personally identifiable information (PII). If no PII is contained in the system, please answer questions in the PIA Summary Tab and then promote the PIA to the Senior Official for Privacy who will authorize the PIA. If this system contains PII, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.

2
Summary of PIA Required Questions

*Is this a new PIA?
No
If this is an existing PIA, please provide a reason for revision:
Annual System Assessment
*1. Date of this Submission:
07/31/12
*2. OPDIV Name:
ATSDR

*3. Unique Project Identifier (UPI) Number for current fiscal year:

UPI: 009-20-01-03-02-9221-00, System ID: 1581

*4. Privacy Act System of Records Notice (SORN) Number (If response to Q.21 is Yes, a SORN number is required for Q.4):

09-19-0001

*5. OMB Information Collection Approval Number:

0923-0041

*6. Other Identifying Number(s):

No

*7. System Name (Align with system item name):

Amyotrophic Lateral Sclerosis Web Portal (ALS)

*9. System Point of Contact (POC). The System POC is the person to whom questions about the system and the responses to this PIA may be addressed:

Point of Contact Information	
POC Name	Oleg I. Muravov

**10. Provide an overview of the system:*

Note: If SSN's(Social Security Numbers) will be collected, maintained (stored), disseminated and/or pass through within any database(s), record(s), file(s) or website(s) hosted by this system you must complete and submit **Attachment A – SSN Elimination or Usage Approval Request located at** http://intranet.cdc.gov/ociso/pandp/policy.html

Note: According to OMB 07-16M, All agencies MUST participate in government-wide effort to eliminate unnecessary use of and explore alternatives to agency use of Social Security Numbers as a personal identifier for both Federal employees and in Federal programs.

The Amyotrophic Lateral Sclerosis Web Portal (ALS) is an online disease registry operated by the Agency for Toxic Substance and Disease Registry (ATSDR) / Office of the Director (OD) / Division of Health Studies (DHS). 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.

The ALS Web Portal will help in completing the following:

- Collect ALS patient information as it relates to the patient's background information, occupational history, military history, smoking and alcohol habits, physical characteristics and activity, family history of disease, and the patient quality of life.
- Make available to the patients and general public educational materials about ALS.
- Identify the incidence and prevalence of ALS in the United States.
- Collect data important to the study of ALS.
- Promote a better understanding of ALS.
- Collect information that is important for research into the genetic and environmental factors that cause ALS.
- Strengthen the ability of a clearing house.
- Collect and disseminate research findings on environmental, genetic, and other causes of ALS and other motor neuron disorders that can be confused with ALS, misdiagnosed as ALS, and in some cases progress to ALS.
- Make available information to patients about research studies for which they may be eligible.
- Maintain information about clinical specialists and clinical trials on therapies.
- Enhance efforts to find treatments and a cure for ALS.

*13. Indicate if the system is new or an existing one being modified:

Existing

*17. Does/Will the system collect, maintain (store), disseminate and/or pass through PII within any database(s), record(s), file(s) or website(s) hosted by this system?

TIP: If the answer to Question 17 is "No" (indicating the system does not contain PII), only the remaining PIA Summary tab questions need to be completed and submitted. If the system does contain PII, the full PIA must be completed and submitted. (Although note that "Employee systems," – i.e., systems that collect PII "permitting the physical or online contacting of a specific individual … employed [by] the **Federal Government – only need to complete the PIA Summary tab.)**

Yes

17a. Is this a GSS PIA included for C&A purposes only, with no ownership of underlying application data? If the response to Q.17a is Yes, the response to Q.17 should be No and only the PIA Summary must be completed. **NOTE: TO BE DETERMINED AND COMPLETED BY OCISO ONLY!!!**
*19. Are records on the system retrieved by 1 or more PII data elements?
Yes
*21. Is the system subject to the Privacy Act? (If the response to Q.19 is Yes, the response to Q.21 must be Yes and a SORN number is required for Q.4)
Yes
*23. If the system shares or discloses PII, please specify with whom and for what purpose(s):
Users will only be allowed to view their own personal information. Any information shared will be general information and not identifiable information.
*30. Please describe in detail: (1) The information the agency will collect, maintain, or disseminate (clearly state if the information contained in the system ONLY represents federal contact data); (2) Why and for what purpose the agency will use the information; (3) Explicitly indicate whether the information contains PII; and (4) Whether submission of personal information is voluntary or mandatory:
(1) The ALS Web Portal collects ALS patient information as it relates to the patient's background information, occupational history, military history, smoking and alcohol habits, physical characteristics and activity, family history of disease, and the patient's quality of life. The ALS Web Portal also collects minimal identifiable information from researchers and the general public such as name, affiliation, email and location. Business addresses are collected in order to mail registry brochures. (2) 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. (3) The ALS Web Portal does contain PII. (4) Submission of personal information is voluntary.
*31. Please describe in detail any processes in place to: (1) 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 the original collection); (2) Notify and obtain consent from individuals regarding what PII is being collected from them; and (3) How the information will be used or shared. (Note: Please describe in what format individuals will be given notice of consent [e.g., written notice, electronic notice, etc.]):

(1) It is required that users give consent to ATSDR to use email as a point of contact. If consent is given, users will be notified by email when major changes occur to the system.

(2) ALS Patients will be notified, before creating an account, how their data will be used in the ALS System. There will be a “Privacy Information” link provided on the registry homepage that will allow users to view an outline of the ALS Privacy Policy. There will also be a standard Privacy Notice and customized Consent Form that allows ALS patients to agree or disagree with ATSDR’s terms. The decision of the patient is voluntary and will determine whether or not an account is created.

(3) PII is not accessible by anyone other than authorized individuals for official business. The ONLY information viewable by the general population is information on ALS and aggregate information. ATSDR may share information with appropriate ATSDR [CDC] administrative staff, scientists, and researchers in order to facilitate the creation of the ALS Registry and further research on ALS.

*32. Does the system host a website? (Note: If the system hosts a website, the Website Hosting Practices section is required to be completed regardless of the presence of PII)

Yes

*37. Does the website have any information or pages directed at children under the age of thirteen?

No

*50. Are there policies or guidelines in place with regard to the retention and destruction of PII? (Refer to the C&A package and/or the Records Retention and Destruction section in SORN)

Records are retained and disposed of in accordance with the ATSDR Comprehensive Records Control Schedule (B-371). 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 legislation. Retention periods vary depending on the type of record. Source documents for computer tapes or disks are 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.

Records may be transferred to a Federal Records Center for storage when no longer needed for evaluation or analysis. Disposal methods include the paper recycling process, burning or shredding hard copy records, and erasing computer tapes and disks.

*54. Briefly describe in detail how the PII will be secured on 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.

ALS Patients can complete surveys, map ALS services, and view educational materials (videos, webinars, and documents) about ALS. The general public will be able to order registry brochures and view educational materials (videos, webinars, and documents) about ALS. All users can edit their own profile information, create their usernames and passwords (with CDC criteria restrictions), and reset/ change their passwords. Users will not be allowed to change their username.

The ALS System Administrator can manage user accounts, manage roles and privileges, and download data. The system administrator panel is only accessible on the ALS Intranet Web Portal via the Administration menu. Users must be approved by ATSDR management and have administrative roles and privileges to access this menu. Also, all tasks performed on the Administration Panel must be pre-approved. The ALS System Administrator is not allowed to perform any administrative tasks outside of CDC grounds and/or access the ALS Web Portal via CITGO or Remote Desktop.

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).

If the response to Question 17 is **"NO"** and Question 32 is **"YES",** you only need to complete the PIA Summary and Website Hosting section (Questions 32 – 40).

If the response to Question 17 is "**YES",** please complete ALL remaining questions.

PIA REQUIRE INFORMATION

1
HHS Privacy Impact Assessment (PIA)

The PIA determines if Personally Identifiable Information (PII) is contained within a system, what kind of PII, what is done with that information, and how that information is protected. Systems with PII are subject to an extensive list of requirements based on privacy laws, regulations, and guidance. The HHS Privacy Act Officer may be contacted for issues related to Freedom of Information Act (FOIA) and the Privacy Act. Respective Operating Division (OPDIV) Privacy Contacts may be contacted for issues related to the Privacy Act. The Office of the Chief Information Officer (OCIO) can be used as a resource for questions related to the administrative, technical, and physical controls of the system. Please note that answers to questions with an asterisk (*) will be submitted to the Office of Management and Budget (OMB) and made publicly available in accordance with OMB Memorandum (M) 03-22.
Note: If a question or its response is not applicable, please answer “N/A” to that question where possible.

2
General Information

*Is this a new PIA?
No
If this is an existing PIA, please provide a reason for revision:
Annual System Assessment
*1. Date of this Submission:
07/31/12
*2. OPDIV Name:
ATSDR
3. Unique Project Identifier (UPI) Number for current fiscal year:
009-20-01-03-02-9221-00, System ID: 1581
*4. Privacy Act System of Records Notice (SORN) Number (If response to Q.21 is Yes, a SORN number is required for Q.4):
09-19-0001
*5. OMB Information Collection Approval Number:
0923-0041
5a. OMB Collection Approval Number Expiration Date:
07-13-2013

*6. Other Identifying Number(s):

No

*7. System Name: (Align with system item name)

Amyotrophic Lateral Sclerosis Web Portal (ALS)

8. System Location: (OPDIV or contractor office building, room, city, and state)

System Location:	
OPDIV or contractor office building	Chamblee 106
Room	B0012
City	Chamblee
State	GA

*9. System Point of Contact (POC). The System POC is the person to whom questions about the system and the responses to this PIA may be addressed:

Point of Contact Information	
POC Name	Oleg I. Muravov

The following information will not be made publicly available:

POC Title	Principal Investigator
POC Organization	ATSDR
POC Phone	770.488.3817
POC Email	oim0@cdc.gov

10. Provide an overview of the system:
Note: If SSN's(Social Security Numbers) will be collected, maintained (stored), disseminated and/or pass through within any database(s), record(s), file(s) or website(s) hosted by this system you must complete and submit **Attachment A – SSN Elimination or Usage Approval Request located at** http://intranet.cdc.gov/ociso/pandp/policy.html
Note: According to OMB 07-16M, All agencies MUST participate in government-wide effort to eliminate unnecessary use of and explore alternatives to agency use of Social Security Numbers as a personal identifier for both Federal employees and in Federal programs.

The Amyotrophic Lateral Sclerosis Web Portal (ALS) is an online disease registry operated by the Agency for Toxic Substance and Disease Registry (ATSDR) / Office of the Director (OD) / Division of Health Studies (DHS). 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.

The ALS Web Portal will help in completing the following:

- Collect ALS patient information as it relates to the patient's background information, occupational history, military history, smoking and alcohol habits, physical characteristics and activity, family history of disease, and the patient quality of life.
- Make available to the patients and general public educational materials about ALS.
- Identify the incidence and prevalence of ALS in the United States.
- Collect data important to the study of ALS.
- Promote a better understanding of ALS.
- Collect information that is important for research into the genetic and environmental factors that cause ALS.
- Strengthen the ability of a clearing house.
- Collect and disseminate research findings on environmental, genetic, and other causes of ALS and other motor neuron disorders that can be confused with ALS, misdiagnosed as ALS, and in some cases progress to ALS.
- Make available information to patients about research studies for which they may be eligible.
- Maintain information about clinical specialists and clinical trials on therapies.
- Enhance efforts to find treatments and a cure for ALS.

SYSTEM CHARACTERIZATION AND DATA CATEGORIZATION

1
System Characterization and Data Configuration

11. Does HHS own the system?

Yes

11a. If no, identify the system owner:

12. Does HHS operate the system? (If the system is operated at a contractor site, the answer should be No)

Yes

12a. If no, identify the system operator:

*13. Indicate if the system is new or an existing one being modified:

Existing

14. Identify the life-cycle phase of this system:

Operations/ Maintenance

15. Have any of the following major changes occurred to the system since the PIA was last submitted?

Please indicate “Yes” or “No” for each category below:	Yes/No
Conversions	No
Anonymous to Non-Anonymous	No
Significant System Management Changes	No
Significant Merging	No
New Public Access	No
Commercial Sources	No
New Interagency Uses	No
Internal Flow or Collection	No
Alteration in Character of Data	No

16. Is the system a General Support System (GSS), Major Application (MA), Minor Application (child) or Minor Application (stand-alone)?

Minor Application (stand-alone)

*17. Does/Will the system collect, maintain (store), disseminate and/or pass through PII within any database(s), record(s), file(s) or website(s) hosted by this system?

Yes

TIP: If the answer to Question 17 is “No” (indicating the system does not contain PII), only the remaining PIA Summary tab questions need to be completed and submitted. If the system does contain PII, the full PIA must be completed and submitted. (Although note that “Employee systems,” – i.e., systems that collect PII “permitting the physical or online contacting of a specific individual … employed [by] the **Federal Government – only need to complete the PIA Summary tab.)**

Please indicate "Yes" or "No" for each PII category. If the applicable PII category is not listed, please use the Other field to identify the appropriate category of PII.

Categories:	Yes/No
Name (for purposes other than contacting federal employees)	Yes
Date of Birth	Yes (month, year)
Social Security Number (SSN) *Note: According to OMB 07-16M, All agencies MUST participate in government-wide effort to eliminate unnecessary use of and explore alternatives to agency use of Social Security Numbers as a personal identifier for both Federal employees and in Federal programs.*	Yes (last 5 digits)
Photographic Identifiers	No
Driver’s License	No
Biometric Identifiers	No
Mother’s Maiden Name	No
Vehicle Identifiers	No
Personal Mailing Address	No
Personal Phone Numbers	Yes
Medical Records Numbers	No
Medical Notes	Yes
Financial Account Information	No
Certificates	No
Legal Documents	No
Device Identifiers	No

Web Uniform Resource Locator(s) (URL)	No
Personal Email Address	Yes
Education Records	No
Military Status	Yes (history)
Employment Status	Yes
Foreign Activities	No
Other	Yes (Race, Gender, Marital Status, Family History, Patient's Quality of Life)

17a. Is this a GSS PIA included for C&A purposes only, with no ownership of underlying application data? If the response to Q.17a is Yes, the response to Q.17 should be No and only the PIA Summary must be completed. **NOTE: TO BE DETERMINED AND COMPLETED BY OCISO ONLY!!!**

18. Please indicate the categories of individuals about whom PII is collected, maintained, disseminated and/or passed through. Note: If the applicable PII category is not listed, please use the Other field to identify the appropriate category of PII. Please answer "Yes" or "No" to each of these choices (NA in other is not applicable).

Categories:	Yes/No
Employees	No
Public Citizen	Yes
Patients	Yes
Business partners/contacts (Federal, state, local agencies)	No
Vendors/Suppliers/Contractors	No
Other	Non-US Citizens

*19. Are records on the system retrieved by 1 or more PII data elements?

Yes

Please indicate "Yes" or "No" for each PII category. If the applicable PII category is not listed, please use the Other field to identify the appropriate category of PII.

Categories:	Yes/No

Name (for purposes other than contacting federal employees)	Yes
Date of Birth	No
Social Security Number (SSN) *Note: According to OMB 07-16M, All agencies MUST participate in government-wide effort to eliminate unnecessary use of and explore alternatives to agency use of Social Security Numbers as a personal identifier for both Federal employees and in Federal programs.*	No
Photographic Identifiers	No
Driver's License	No
Biometric Identifiers	No
Mother's Maiden Name	No
Vehicle Identifiers	No
Personal Mailing Address	No
Personal Phone Numbers	No
Medical Records Numbers	No
Medical Notes	No
Financial Account Information	No
Certificates	No
Legal Documents	No
Device Identifiers	No
Web URLs	No
Personal Email Address	Yes
Education Records	No
Military Status	No
Employment Status	No
Foreign Activities	No
Other	Security Questions

20. Are 10 or more records containing PII maintained, stored or transmitted/passed through this system?

Yes

*21. Is the system subject to the Privacy Act? (If the response to Q.19 is Yes, the response to Q.21 must be Yes and a SORN number is required for Q.4)

Yes

21a. If yes but a SORN has not been created, please provide an explanation.

INFORMATION SHARING PRACTICES

1
Information Sharing Practices

22. Does the system share or disclose PII with other divisions within this agency, external agencies, or other people or organizations outside the agency?

No

Please indicate "Yes" or "No" for each category below:	Yes/No
Name (for purposes other than contacting federal employees)	No
Date of Birth	No
Social Security Number (SSN) *Note: According to OMB 07-16M, All agencies MUST participate in government-wide effort to eliminate unnecessary use of and explore alternatives to agency use of Social Security Numbers as a personal identifier for both Federal employees and in Federal programs.*	No
Photographic Identifiers	No
Driver's License	No
Biometric Identifiers	No
Mother's Maiden Name	No
Vehicle Identifiers	No
Personal Mailing Address	No
Personal Phone Numbers	No
Medical Records Numbers	No
Medical Notes	No
Financial Account Information	No
Certificates	No
Legal Documents	No
Device Identifiers	No
Web URLs	No
Personal Email Address	No
Education Records	No
Military Status	No
Employment Status	No
Foreign Activities	No

Other	No

*23. If the system shares or discloses PII please specify with whom and for what purpose(s):
N/A. The ALS Web Portal does not share or disclose PII with any other entity.
24. If the PII in the system is matched against PII in one or more other computer systems, are computer data matching agreement(s) in place?
No
25. Is there a process in place to notify organizations or systems that are dependent upon the PII contained in this system when major changes occur (i.e., revisions to PII, or when the system is replaced)?
N/A. There are no organizations or system dependent on the PII contained in the ALS Web Portal.
26. Are individuals notified how their PII is going to be used?
Yes
26a. If yes, please describe the process for allowing individuals to have a choice. If no, please provide an explanation.
Individuals are notified during the self-registration process.
27. Is there a complaint process in place for individuals who believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate?
Yes
27a. If yes, please describe briefly the notification process. If no, please provide an explanation.
Users can contact ATSDR via the contact information provided on the ALS website or SORN if any issues occur.
28. Are there processes in place for periodic reviews of PII contained in the system to ensure the data’s integrity, availability, accuracy and relevancy?
Yes
28a. If yes, please describe briefly the review process. If no, please provide an explanation.
The system data will be reviewed annually during the Annual Self Assessments or Recertification process. The system will be reviewed also through the Change Management process.
29. Are there rules of conduct in place for access to PII on the system?
Yes

Please indicate "Yes," "No," or "N/A" for each category. If yes, briefly state the purpose for each user to have access:

Users with access to PII	Yes/No/N/A	Purpose
User	Yes	To access personal account information only
Administrators	Yes	To manage data, manage users, manage roles and privileges and download data
Developers	Yes	To manage code
Contractors	Yes	To manage code, database, customer support and testing
Other	Yes	FTE: to manage ALS data, match it with the National ALS Registry data.

*30. Please describe in detail: (1) The information the agency will collect, maintain, or disseminate (clearly state if the information contained in the system ONLY represents federal contact data); (2) Why and for what purpose the agency will use the information; (3) Explicitly indicate whether the information contains PII; and (4) Whether submission of personal information is voluntary or mandatory:

(1) The ALS Web Portal collects ALS patient information as it relates to the patient's background information, occupational history, military history, smoking and alcohol habits, physical characteristics and activity, family history of disease, and the patient's quality of life. The ALS Web Portal also collects minimal identifiable information from researchers and the general public such as name, affiliation, email and location. Business addresses are collected in order to mail registry brochures.

(2) 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.

(3) The ALS Web Portal does contain PII.

(4) Submission of personal information is voluntary.

*31. Please describe in detail any processes in place to: (1) 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 the original collection); (2) Notify and obtain consent from individuals regarding what PII is being collected from them; and (3) How the information will be used or shared. (Note: Please describe in what format individuals will be given notice of consent [e.g., written notice, electronic notice, etc.])
(1) It is required that users give consent to ATSDR to use email as a point of contact. If consent is given, users will be notified by email when major changes occur to the system. (2) ALS Patients will be notified, before creating an account, how their data will be used in the ALS System. There will be a “Privacy Information” link provided on the registry homepage that will allow users to view an outline of the ALS Privacy Policy. There will also be a standard Privacy Notice and customized Consent Form that allows ALS patients to agree or disagree with ATSDR’s terms. The decision of the patient is voluntary and will determine whether or not an account is created. (3) PII is not accessible by anyone other than authorized individuals for official business. The ONLY information viewable by the general population is information on ALS and aggregate information. ATSDR may share information with appropriate ATSDR [CDC] administrative staff, scientists, and researchers in order to facilitate the creation of the ALS Registry and further research on ALS.

WEBSITE HOSTING PRACTICES

1
Website Hosting Practices

*32. Does the system host a website? (Note: If the system hosts a website, the Website Hosting Practices section is required to be completed regardless of the presence of PII)

Yes

Please indicate "Yes" or "No" for each type of site below. If the system hosts both Internet and Intranet sites, indicate "Yes" for "Both" only.	Yes/ No	If the system hosts an Internet site, please enter the site URL. Do not enter any URL(s) for Intranet sites.
Internet		http://wwwn.cdc.gov/ALS/Default.aspx
Intranet		
Both	Yes	

33. Does the system host a website that is accessible by the public and does not meet the exceptions listed in OMB M-03-22?

Note: OMB M-03-22 Attachment A, Section III, Subsection C requires agencies to post a privacy policy for websites that are accessible to the public, but provides three exceptions: (1) Websites containing information other than "government information" as defined in OMB Circular A-130; (2) Agency intranet websites that are accessible only by authorized government users (employees, contractors, consultants, fellows, grantees); and (3) National security systems defined at 40 U.S.C. 11103 as exempt from the definition of information technology (see section 202(i) of the E-Government Act.).

Yes

34. If the website does not meet one or more of the exceptions described in Q. 33 (i.e., response to Q. 33 is "Yes"), a website privacy policy statement (consistent with OMB M-03-22 and Title II and III of the E-Government Act) is required. Has a website privacy policy been posted?
(Note: A website privacy policy is required for Internet sites only.)

Yes

35. If a website privacy policy is required (i.e., response to Q. 34 is "Yes"), is the privacy policy in machine-readable format, such as Platform for Privacy Preferences (P3P)?
(Note: Privacy policy in machine-readable format is required for Internet sites only.)

Yes

35a. If no, please indicate when the website will be P3P compliant:

36. Does the website employ tracking technologies?

Yes

Please indicate "Yes", "No", or "N/A" for each type of cookie below:	Yes/No/N/A
Web Bugs	No
Web Beacons	No
Session Cookies	Yes
Persistent Cookies	No
Other	No

*37. Does the website have any information or pages directed at children under the age of thirteen?

No

37a. If yes, is there a unique privacy policy for the site, and does the unique privacy policy address the process for obtaining parental consent if any information is collected?

38. Does the website collect PII from individuals?

Yes

Please indicate "Yes" or "No" for each category below:	Yes/No
Name (for purposes other than contacting federal employees)	Yes
Date of Birth	Yes (month, year)
Social Security Number (SSN) *Note: According to OMB 07-16M, All agencies MUST participate in government-wide effort to eliminate unnecessary use of and explore alternatives to agency use of Social Security Numbers as a personal identifier for both Federal employees and in Federal programs.*	Yes (last 5 digits)
Photographic Identifiers	No
Driver's License	No
Biometric Identifiers	No
Mother's Maiden Name	No
Vehicle Identifiers	No
Personal Mailing Address	No
Personal Phone Numbers	Yes

Medical Records Numbers	No
Medical Notes	No
Financial Account Information	No
Certificates	No
Legal Documents	No
Device Identifiers	No
Web URLs	No
Personal Email Address	Yes
Education Records	No
Military Status	Yes (history)
Employment Status	Yes
Foreign Activities	No
Other	Yes (Race, Gender, Marital Status, Family History, Patient's Quality of Life)

39. Are rules of conduct in place for access to PII on the website?

Yes

40. Does the website contain links to sites external to HHS that owns and/or operates the system?

Yes

40a. If yes, note whether the system provides a disclaimer notice for users that follow external links to websites not owned or operated by HHS.

The system provides a disclaimer notice and pop-up for users that follow external links.

ADMINISTRATIVE CONTROLS

1
Administrative Controls

Note: This PIA uses the terms "Administrative," "Technical" and "Physical" to refer to security control questions—terms that are used in several Federal laws when referencing security requirements.

41. Has the system been certified and accredited (C&A)?

Yes
41a. If yes, please indicate when the C&A was completed (Note: The C&A date is populated in the System Inventory form via the responsible Security personnel):
ATO Date: September 9, 2010
41b. If a system requires a C&A and no C&A was completed, is a C&A in progress?
42. Is there a system security plan for this system?
Yes
43. Is there a contingency (or backup) plan for the system?
Yes
44. Are files backed up regularly?
Yes
45. Are backup files stored offsite?
Yes
46. Are there user manuals for the system?
Yes
47. Have personnel (system owners, managers, operators, contractors and/or program managers) using the system been trained and made aware of their responsibilities for protecting the information being collected and maintained?
Yes
48. If contractors operate or use the system, do the contracts include clauses ensuring adherence to privacy provisions and practices?
Yes
49. Are methods in place to ensure least privilege (i.e., “need to know” and accountability)?
Yes
49a. If yes, please specify method(s):
SQL read/write permissions controlled by user roles and privileges. Active Directory controls administrator access. E-Authentication control for external users.
*50. Are there policies or guidelines in place with regard to the retention and destruction of PII? (Refer to the C&A package and/or the Records Retention and Destruction section in SORN):

Yes

50a. If yes, please provide some detail about these policies/practices:

Records are retained and disposed of in accordance with the ATSDR Comprehensive Records Control Schedule (B-371). 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 legislation. Retention periods vary depending on the type of record. Source documents for computer tapes or disks are 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.

Records may be transferred to a Federal Records Center for storage when no longer needed for evaluation or analysis. Disposal methods include the paper recycling process, burning or shredding hard copy records, and erasing computer tapes and disks.

1
Technical Controls

51. Are technical controls in place to minimize the possibility of unauthorized access, use, or dissemination of the data in the system?

Yes

Please indicate “Yes” or “No” for each category below:	Yes/No
User Identification	Yes
Passwords	Yes
Firewall	Yes
Virtual Private Network (VPN)	No
Encryption	Yes
Intrusion Detection System (IDS)	Yes
Common Access Cards (CAC)	Yes
Smart Cards	Yes
Biometrics	No
Public Key Infrastructure (PKI)	No

52. Is there a process in place to monitor and respond to privacy and/or security incidents?

Yes

52a. If yes, please briefly describe the process:

In accordance with OMB M-06-19, CDC must report all incidents involving PII in electronic or physical form to the Secure One Communications Center (SOCC) within one hour.

PHYSICAL ACCESS

1
Physical Access

53. Are physical access controls in place?

Yes

Please indicate “Yes” or “No” for each category below:	Yes/No
Guards	Yes
Identification Badges	Yes
Key Cards	Yes
Cipher Locks	No
Biometrics	No
Closed Circuit TV (CCTV)	Yes

*54. Briefly describe in detail how the PII will be secured on 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 Web Portal "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.

ALS Patients can complete surveys, map ALS services, and view educational materials (videos, webinars, and documents) about ALS. The general public will be able to order registry brochures and view educational materials (videos, webinars, and documents) about ALS. All users can edit their own profile information, create their usernames and passwords (with CDC criteria restrictions), and reset/ change their passwords. Users will not be allowed to change their username.

The ALS System Administrator can manage user accounts, manage roles and privileges, and download data. The system administrator panel is only accessible on the ALS Intranet Web Portal via the Administration menu. Users must be approved by ATSDR management and have administrative roles and privileges to access this menu. Also, all tasks performed on the Administration Panel must be pre-approved. The ALS System Administrator is not allowed to perform any administrative tasks outside of CDC grounds and/or access the ALS Web Portal via CITGO or Remote Desktop.

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).

APPROVAL/DEMOTION

1
System Information

System Name:	

2
PIA Reviewer Approval/Promotion or Demotion

Promotion/ Demotion:	
Comments:	
Approval/ Demotion Point of Contact:	
Date:	

3
Senior Official for Privacy Approval/Promotion or Demotion

Promotion/ Demotion:	
Comments:	

4
OPDIV Senior Official for Privacy or Designee Approval

Please print the PIA and obtain the endorsement of the reviewing official below. Once the signature has been collected, retain a hard copy for the OPDIV's records. Submitting the PIA will indicate the reviewing official has endorsed it
This PIA has been reviewed and endorsed by the OPDIV Senior Official for Privacy or Designee (Name and Date):
Name: _____ **Date:** _____
Name: / **Date:**

5

Department Approval to Publish to the Web

Approved for web publishing	
Date Published:	
Publicly posted PIA URL or no PIA URL explanation:	