Privacy Impact Assessment Form

v 1.47.4

Question	Answer	
1 OPDIV:	NIH	
2 PIA Unique Identifier:	P-7517519-327592	
2a Name:	NCI Cancer Information Service Contact Center	
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 Telecommunications Specialist POC Name Robert Zablocki POC Organization NIH/NCI/OCPL POC Email zablocb@mail.nih.gov POC Phone 240-793-8642	
7 Is this a new or existing system?	○ New ◉ Existing	
8 Does the system have Security Authorization (SA)?	◉ Yes ○ No	
8a Date of Security Authorization	Aug 7, 2023	

9	Indicate the following reason(s) for updating this PIA. Choose from the following options.	☒ PIA Validation (PIA Refresh/Annual Review) ☐ Significant System Management Change ☐ Anonymous to Non-Anonymous ☐ Alteration in Character of Data ☐ New Public Access ☐ New Interagency Uses ☐ Internal Flow or Collection ☐ Conversion ☐ Commercial Sources
10	Describe in further detail any changes to the system that have occurred since the last PIA.	The following responses have changed since the last PIA was approved: Point of Contact number updated OMB information collection expiration date updated Security authorization date updated
11	Describe the purpose of the system.	The Cancer Information Service Contact Center (CIS) is a public service provided by the National Cancer Institute (NCI) that provides the general public with information concerning cancer causes, prevention and answers to general questions. The service comprises telephone, web, chat, e-mail, and e-referral methods to communicate.
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.)	Through the following access channels phones, chat, e-mail, mail, social media and Kno2, Veteran Administration's (VA) preferred secure file transfer provider, clients may voluntarily provide Personally Identifiable Information (PII) and other information including name, email address, phone number, education records, mailing address, age, sex, ethnicity, race and household income during the inquiry response, materials ordering, or research participation processes. NCI accesses the system with a user name and password to administer. Chats are kept and purged in compliance with the records retention schedule.
13	Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.	The Cancer Information Service is a public service provided by the National Cancer Institute (NCI) that provides the general public with information concerning cancer causes, prevention and answers to general questions. The service comprises telephone, web, chat, e-mail, and e-referral methods to communicate. Through the following access channels phones, chat, e-mail, mail, social media and Kno2, Veteran Administration's (VA) preferred secure file transfer provider, clients may voluntarily provide Personally Identifiable Information (PII) and other information including name, email address, phone number, education records, mailing address, age, sex, ethnicity, race and household income during the inquiry response, materials ordering, or research participation processes. NCI accesses the system with a user name and password to administer. Chats are kept and purged in compliance with the records retention schedule.
14	Does the system collect, maintain, use or share **PII**?	◉ Yes ○ No

15	Indicate the type of PII that the system will collect or maintain.	☐ Social Security Number ☐ Date of Birth

Checkbox list:

☐ 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

age, sex, ethnicity, race

household income

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?

500-4,999

---

18 For what primary purpose is the PII used?

Personally Identifiable Information (PII) is collected in the about interactions with the public. Name, mailing address, and e-mail address information is used for fulfillment of publication requests.

The calls recorded could contain PII data (name, address, email, phone, age and sex) if the client requests to have material sent to them.

---

19 Describe the secondary uses for which the PII will be used (e.g. testing, training or research)

Secondary uses of PII are for training and by NCI & Contact Center Supervisors Quality Assurance (QA) evaluators to ensure call quality.

---

20 Describe the function of the SSN.

Not Applicable (NA)

20a Cite the **legal authority** to use the SSN.

NA

| 21 | Identify **legal authorities** governing information use and disclosure specific to the system and program. | Public Health Service Act. (42 U.S.C. 241, 242, 248, 281, 282, 284, 285a-285q, 287, 287b, 287c, 289a, 289c, and 44 U.S.C. 3101) | |

| 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: 09-90-1901, HHS Correspondence, Comment, Customer Service, and Contact List Records
 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. | 0925-0208; Expiration Date: 11/30/2025 |

| 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.	On the LiveHelp chat welcome page, a written privacy notice is posted letting users know the service is anonymous and asking not to send PII during the chat. For PII collected during a phone call, Information Specialists read a statement to clients that information provided will be kept confidential, and research studies contain their own additional informed consent statements that are read to clients. Additionally, CIS is working to add a Privacy Act Statement the the sites.
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.	CIS Specialists inform clients that information provided will be kept confidential. Research studies contain their own additional informed consent statements that are read to clients. Individuals can choose not to provide their information. However, in doing so, they will not be able to have material shipped to them.
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.	CIS Specialists inform clients that information provided will be kept confidential and obtain consent before the call. Research studies contain their own additional informed consent statements that are read to clients. Individuals can choose not to provide their information. However, in doing so, they will not be able to have material shipped to them.
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.	Clients may contact the Cancer Information Service (CIS) at 800-422-6237 or nciinfo@nih.gov. The CIS would refer the complaint to the Branch Chief for the Contact Center and Patient Inquiries Branch.
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.	Validation is run on city/state/ZIP Code combinations entered into CIS at the time of data entry to ensure accuracy. Records are reviewed when QA evaluations are done on a monthly bases.

31	Identify who will have access to the PII in the system and the reason why they require access.	☒ Users	Users have access to PII to respond to inquiries and correspondence with the public. QA evaluators have acccess as part of their quality reviews.
		☒ Administrators	Administrators have access to troubleshoot issues and for general maintenance.
		☒ Developers	Administrators have access to troubleshoot issues and for general maintenance.
		☒ Contractors	Third party contractors have access to handle the daily operations of the call center. Direct contractors have access as NCI employees to help with
		☒ Others	Researchers reviewing data provided by clients volunteering to participate in research studies.

32	Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	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.
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.	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.
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.	According to NIH policy, all personnel who manage or operate NIH applications must successfully complete annual security awareness training. There are five categories of mandatory IT training (Information Security, Counterintelligence, Privacy Awareness, Records Management and Emergency Preparedness). Training is completed on the http://irtsectraining.nih.gov site with valid NIH credentials.
35	Describe training system users receive (above and beyond general security and privacy awareness training).	Oracle promotes security awareness and educates employees through quarterly newsletters, ad hoc security awareness campaigns, and security-related corporate emails. Each employee who handles data is required to complete a data privacy awareness training course. The course instructs employees on the definitions of data privacy and personal data, recognizing risks relating to personal data, understanding their responsibilities towards data, and reporting any suspected privacy violations. Employees handling data are also required to complete training in corporate ethics. Additionally, employees involved in development of custom code are required to attend secure coding training.
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.	Schedule 11-202, Communications and Agency History. Disposition Authority: DAA-GRS-2016-0005-0002. Destroy when 90 days old, but longer retention is authorized if required for business use.

38	Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.	Administrative: CIS maintains a comprehensive list of Standard Operating Procedures, guidance, and policies for the handling of CIS data and system use. Contingency and Configuration Management Plans have been developed, and are updated on a regular basis to guide management of CIS. The CIS System Security Plan contains detailed documentation of all selected controls that describe the access controls, system and communication, and the physical and environmental families. These controls detail the protections in place for CIS, and document the processes and procedures that are followed in the administration of the system. Technical: Access controls are in place to ensure users can only access data required for their daily job functions. All inbound and outbound communications are monitored by firewall logs and intrusion detection systems. File system-level encryption is used to encrypt all customer data at rest adn during transmission, including all file attachments. Physical: Authorization is required to enter Oracle facilities and access is monitored. Official identification must be worn while onsite. Visitors must sign a visitor's register and be escorted when on the premises. Possession of keys/access cards and the ability to access locations is managed based upon role requirements. Staff leaving Oracle employment must return keys/cards. Continuous monitoring is done by Closed Caption Television. Physical barriers are designed to prevent persons and vehicles from unauthorized entry. Entrances are manned 24 hours a day, 365 days a year by security guards who perform visual identity recognition and visitor escort management.	
39	Identify the publicly-available URL:	https://livehelp.cancer.gov http://supportorgs.cancer.gov http://www.cancer.gov/global/contact/email-us	
40	Does the website have a posted privacy notice?	⦿ Yes ○ No	
	format?	⦿ Yes ○ No	
41	Does the website use web measurement and customization technology?	⦿ Yes ○ No	

	Technologies	Collects PII?
☐	Web beacons	◯ Yes ◯ No
☐	Web bugs	◯ Yes ◯ No
☒	Session Cookies	◯ Yes ◉ No
☐	Persistent Cookies	◯ Yes ◯ No
Other... [ ]		◯ Yes ◯ No

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)

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	While the CIS doesn't reside within an NIH boundary, third party contractors must still follow Authority to Operate standards and processes. As well as obtaining authorization approval. Specific and defined privacy and security control thresholds and expectations controlled by the third party are established during the acquisitions and contracting process to assure compliance with Federal requirements, and the continuous monitoring of the agreed upon risk posture.

OPDIV Senior Official for Privacy Signature	Dustin B. Close -S	Digitally signed by Dustin B. Close -S Date: 2024.09.13 08:58:44 -04'00'	HHS Senior Agency Official for Privacy	Bridget M. Guenther -S	Digitally signed by Bridget M. Guenther -S Date: 2024.10.31 11:02:00 -04'00'