NCI/Office of Communications and Public Liaison

APPENDIX 4

PRIVACY IMPACT ASSESSMENT

Privacy Impact Assessment

Save

Privacy Impact Assessment Form

Status	Draft	Form Number	Read Only	Form Date	Read Only

	Question	Answer
1	OPDIV:	Read Only - OPDIV
2	PIA Unique Identifier:	Read Only- PIA Unique ID
2a	Name:	Read Only-Name
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: 240-276-6672
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	Jul 28, 2014
8b	Planned Date of Security Authorization	N/A ☐ Not Applicable

Save

8c	Briefly explain why security authorization is not required	N/A	
9	Indicate the following reason(s) for updating this PIA. Choose from the following options.	☒ PIA Validation (PIA Refresh/Annual Review) ☐ Anonymous to Non-Anonymous ☐ New Public Access ☒ Internal Flow or Collection ☐ Commercial Sources	☐ Significant System Management Change ☐ Alteration in Character of Data ☐ New Interagency Uses ☐ Conversion Other...
10	Describe in further detail any changes to the system that have occurred since the last PIA.	N/A	
11	Describe the purpose of the system.	The Cancer Information Service is a public service provided by the National Cancer Institute that provides the general public with information concerning cancer causes, prevention and answers to general questions. The service comprises telephone, web, chat, and e-mail 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 various access channels (chat, e-mail, mail, and phone) clients may voluntarily provide PII and other information including name, address, phone number, e-mail address, health information, and demographic information during the inquiry response, materials ordering, or research participation processes.	
13	Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.	The information collected by the system is only used to provide the requested services to the client, or shared with researchers during the course of a research study. Aggregate information that is not personally identifiable is used to describe and improve our services. Contact information is purged on a rolling basis every 90 days. The calls recording will likely contain PII data (name, address, email, phone, age and gender) if the client requests to have material sent to them. It is a call monitoring system that records calls and is used only by NCI & Contact Center Supervisors QA evaluators to ensure call quality.	
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	Other...
		Age & Gender	Other...
		City, State & Zip code	Other...

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?	PII collected in the Oracle Right Now system about an interaction with the public may pass through name, mailing address, and e-mail address information to the Oracle RightNow CX system for fulfillment of publication requests. The calls recorded will likely contain PII data (name, address, email, phone, age and gender) if the client requests to have material sent to them. It is a call monitoring system that records calls and is used only by NCI & Contact Center Supervisors QA evaluators to ensure call quality.

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

20	Describe the function of the SSN.	N/A

21	Identify **legal authorities** governing information use and disclosure specific to the system and program.	N/A

22	Are records on the system retrieved by one or more PII data elements?	⦿ Yes ◯ No

Save

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:	09-25-0208
		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 - 12/31/2018

24	Is the PII shared with other organizations?	⦿ Yes ◯ No

24a	Identify with whom the PII is shared or disclosed and for what purpose.	☒ Within HHS	PII collected in the Oracle RightNow...
		☒ Other Federal Agency/Agencies	PII collected in the Oracle RightNow...
		☐ State or Local Agency/Agencies	
		☐ Private Sector	

24b	Describe any agreements in place that authorizes the information sharing or disclosure (e.g. Computer Matching Agreement, Memorandum of Understanding (MOU), or Information Sharing Agreement (ISA)).	Oracle's Chief Privacy Officer, legal department, and OracleCorp...
24c	Describe the procedures for accounting for disclosures	Oracle's Chief Privacy Officer, legal department, and OracleCorp...

Save

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.
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.	This contact information is only taken and used at the request of the client, who wishes additional information in follow up to their initial contact. Before information is stored in theOracle RightNow CX, Information 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.
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.	Individual public users of the Cancer Information Service cannot be contacted when major changes are made to the Oracle Right Now and its applications because contact information is purged on a rolling basis every 90 days.
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. The CIS would refer the complaint to Mary Anne Bright, Contact Center and Patient Inquiries Branch at 240-276-6647.
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 the Oracle RightNow CX at the time of data entry to ensure accuracy. Oracle RightNow CX records are reviewed when monitoring Contact Center interactions for quality.
31	Identify who will have access to the PII in the system and the reason why they require access.	☒ Users Oracle, data entry and response to inqu ☒ Administrators Troubleshooting, order upload to fulfill ☒ Developers Troubleshooting as needed. ☒ Contractors Shipping vendors to deliver orders. Sof ☒ Others Researchers reviewing data provided b

Save

32	Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Access to Oracle Right Now services and the rights for individual user accounts are governed by the role-based access control model within services. Customer service administrators are responsible for managing end users within the application. Within Oracle, terminations are processed automatically through the Oracle Human Resources Management System. The terminated person's manager is responsible for submitting the voluntary termination forms through Oracle's human resources service application. Human Resources staff process involuntary terminations. After a termination is processed, automated notifications are issued to necessary parties based on the effective date of the termination. Access to systems is terminated at this time. Any transfers of Oracle Right Now operations personnel to a different department (outside of Oracle Cloud operations) will result in the removal of VPN access and system access into Oracle Cloud environments. Access to Calabrio Call Recording application is role-based and NCIDC program management determines the appropriate role/level of access for staff based on job requirements and responsibilities.	
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 Oracle Service Cloud defines user authorization permissions based on the user role (Profile) associated to their user account. A single user role is associated to a user account and is maintained by an administrator who has the security permission to maintain user accounts and user profiles. When defining the user profile the administrator is able to define the granular access for the data objects which are available to the user profile. They will define the create, update, and delete permissions along with specific object permissions for the standard application objects: • Contacts • Organizations • Incidents • Answers • Tasks • Opportunities • Outreach • Feedback • Analytics They will also be able to define the permissions to access custom business objects that are created within the site. Calabrio Call Recording, Role-based access is assigned to users, with only the necessary access and permissions. Access control to the information system is enforced through unique UserID and password.	

Save

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.	Oracle employees are required to complete Ethics training as well as Information Protection Awareness training upon hiring and on a reccurring basis throughout the term of their employment. The Information Protection Awareness course instructs employees on their obligations under the various central Oracle privacy and security policies (such as the Information Protection Policy, Acceptable Use Policy, Security Breach Disclosure Policy and the Services Privacy Policy). This course also trains employees on data privacy principles as well as data handling practices that may apply to their jobs at Oracle and are required by company policy, including those related to notice, consent, use, access, integrity, sharing, retention, security and disposal of data. Calabrio employees take mandated Annual Security Awareness Training.
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. For details, refer to the following links. Oracle Cloud Services: http://www.oracle.com/us/corporate/contracts/cloud-services/index.html Oracle Enterprise Hosting and Delivery Policies: http://www.oracle.com/us/corporate/contracts/cloud-ent-hosting-del-policies-1881438.pdf Oracle Hosting and Delivery Policies: http://www.oracle.com/us/corporate/contracts/cloud-hosting-delivery-policies-1881437.pdf Calabrio employees take mandated Annual Security Awareness 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.	Contact records, which contain the bulk of the system's PII are purged on a rolling basis every 90 days. Chat and email transcripts, which may contain PII voluntarily provided by clients are retained. After 90 days, only system administrators have the ability to view them. Calabrio Call recording application sets the retention period per The Oracle Service Cloud follows FISMA and currently provides a FISMA Moderate Government Cloud including a SA&A package. Administrative Controls Oracle's access control policy is set forth in Oracle's Logical Access Control Policy, Version 1.2 dated 26 Nov 2012. The Logical Access Controls Policy sets forth the requirements for information owners to define, document, and enforce logical access controls for the information systems for which they have responsibility and which process Confidential

Page 7 of 10

Save

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

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

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)	Technologies	Collects PII?
		☐ 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

REVIEWER QUESTIONS: The following section contains Reviewer Questions which are not to be filled out unless the user is an OPDIV Senior Officer for Privacy.

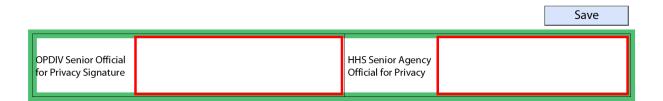|	Reviewer Questions	Answer
1	Are the questions on the PIA answered correctly, accurately, and completely?	◯ Yes ◯ No
Reviewer Notes		
2	Does the PIA appropriately communicate the purpose of PII in the system and is the purpose justified by appropriate legal authorities?	◯ Yes ◯ No
Reviewer Notes		
3	Do system owners demonstrate appropriate understanding of the impact of the PII in the system and provide sufficient oversight to employees and contractors?	◯ Yes ◯ No
Reviewer Notes		

Save

Reviewer Questions	Answer
4 Does the PIA appropriately describe the PII quality and integrity of the data?	○ Yes ○ No
Reviewer Notes	
5 Is this a candidate for PII minimization?	○ Yes ○ No
Reviewer Notes	
6 Does the PIA accurately identify data retention procedures and records retention schedules?	○ Yes ○ No
Reviewer Notes	
7 Are the individuals whose PII is in the system provided appropriate participation?	○ Yes ○ No
Reviewer Notes	
8 Does the PIA raise any concerns about the security of the PII?	○ Yes ○ No
Reviewer Notes	
9 Is applicability of the Privacy Act captured correctly and is a SORN published or does it need to be?	○ Yes ○ No
Reviewer Notes	
10 Is the PII appropriately limited for use internally and with third parties?	○ Yes ○ No
Reviewer Notes	
11 Does the PIA demonstrate compliance with all Web privacy requirements?	○ Yes ○ No
Reviewer Notes	
12 Were any changes made to the system because of the completion of this PIA?	○ Yes ○ No
Reviewer Notes	
General Comments	

Save

| OPDIV Senior Official for Privacy Signature | | HHS Senior Agency Official for Privacy | |

PDF Locked Fields

NIH NCI CIS Cancer Information Service

1. NIH/NCI/OCPL

2a. OCPL Cancer Information Service (CIS)

3b. Is this a FISMA-Reportable system? No

5. Identify the operator: Contractor

7. Is this a new or existing system? Existing

8. Does the system have security authorization? Yes