Privacy Impact Assessment Form v 3.0
Status Form Number Form Date
Question Answer

1. OPDIV: Substance Abuse and Mental Health Services Administration

2. PIA Unique Identifier (UID):

2a. Name: Suicide Prevention Data Center (SDPC)

3. Which of the following objects does this PIA Cover?
☐ **General Support System (GSS)**
☐ **Major Application**
☒ **Minor Application (stand-alone)**
☐ **Minor Application (child)**
☒ **Electronic Information Collection**
☐ **Unknown**

3a. Identify the Enterprise Life-Cycle Phase of the System:
Core system is in Operations & Maintenance with occasional functionality updates

3b. Is this a FISMA Reportable System?
☒ Yes
☐ No

4. Does the system include a publicly available Web interface?
☒ Yes
☐ No

5. Identify the Operator
☐ Agency
☒ Contractor

6. Point of Contact (POC):
POC Title - Principal Investigator/Project Director
POC Name – Christine Walrath
POC Organization – ICF International
POC Email - Christine.Walrath@icfi.com
POC Phone – 646-695-8154

7. Is the system/collection a new or existing system?
Existing – The Suicide Prevention Data Center is an existing system with modifications to accommodate new functionality.

8. Does the System have Security Authorization (SA)?
☒ Yes

☐ No

9. Indicate the following reason(s) for this update

☒ 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 the changes that have occurred since the last PIA.

11. Describe the purpose of the system.

The Suicide Prevention Data Center (SDPC) is a Web-based data collection and management system used to facilitate data collection by program staff, program participants, key stakeholders, students, and Campus faculty/staff. The SPDC will serve two functions: (1) as a data entry tool for program staff and cross-site evaluation staff to enter cross-site evaluation information or data elements, and (2) as a data collection tool for administering Web-based surveys to respondents. All cross-site evaluation data obtained either through direct entry by program and/or evaluation staff or through Web-based surveys will be stored in the SPDC. The Web-based data collection and management system reduces evaluation burden for the grantees and allows ease of access to data for program personnel and cross-site evaluation team members.

12. Describe the type of information the system will collect, maintain (store), or share (Subsequent questions will identify if this information is PII and the specific data elements.)

The SPDC collects and stores the following types of information:

- User and potential respondent contact information
- GLS cross-site evaluation information and data elements
- Web-based survey data

Aggregate data tables are shared with GLS grantees and SAMHSA project officers. GLS grantees have access to data downloads of data collected for their site only. Contact information for potential survey respondents are only shared with data collection activity leads (ICF contractor staff) and the SPDC Administrator.

13. Provide an overview of the system and describe the information it will collect, maintain (store), disseminate and/or pass through it

The Suicide Prevention Data Center (SPDC) is an Internet-based data collection and management system developed by ICF International for the cross-site evaluation of the Garrett Lee Smith Youth Suicide Prevention and Early Intervention Program (GLS Suicide Prevention Program. The SPDC has the capacity to:

- enable users to upload cross-site data and enter data via Web-based surveys,
- store cross-site evaluation data,
- provide access to cross-site evaluation data sets and reports,
- provide access to cross-site evaluation instruments,
- provide links to additional cross-site evaluation resources.

PII will be collected for the following activities:

- Coalition Profile (CP) – contact information for organizations participating in grantee suicide prevention coalition.
- SPDC users - contact information to complete their SPDC user profile
- Short Messaging Service Survey (SMSS) – contact information from Students who provide their name and phone number for SMSS

14. Does the system collect, maintain, use or share PII?

☒ Yes
☐ No

15. Indicate the type of PII.

☐ 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 – zip code only
☒ 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

16. Indicate the categories of individuals about whom PII is collected, maintained, disseminated and/or passed through

- ☐ Employees
- ☒ Public Citizens
- ☐ Business Partners/Contacts (Federal, state, local agencies)
- ☐ Vendors/Suppliers/Contractors
- ☐ Patients
- ☐ Other

17. How many individuals' PII is in the system?

<100
100-499
500-4,999
5,000-9,999
50,000-99,999
100,000-1,000,000
<1,000,000

18. For what primary purpose is the PII used?

The email and telephone contact information gathered for two data collection activities (CP and SMSS) via the SPDC is used to send URL links to surveys for potential respondents. The contact information collected as part of the SPDC users function is stored in the system, and is not used for any other purpose.

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

N/A

20. Describe the function of the SSN.

N/A This system does not collect SSNs.

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

N/A This system does not collect SSNs.

21. Identify legal authorities governing information use and disclosure specific to the system and program

The Garrett Lee Smith Memorial Act (GLSMA), passed by Congress in October 2004, was the first legislation to provide funding specifically for State/Tribal and Campus Suicide Prevention programs. This legislation sets aside funding for states, tribes, and institutions of higher education to develop, evaluate, and improve early intervention and suicide prevention programs, and mandates that the effectiveness of programs be evaluated and reported to Congress. Evaluation data are gathered via the cross-site evaluation of the Garrett Lee Smith (GLS) Memorial Youth Suicide Prevention and Early Intervention Program—the GLS State/Tribal Suicide Prevention Program (State/Tribal Suicide Prevention Program) and the GLS Campus Suicide Prevention Program (Campus Suicide Prevention Program). The Substance Abuse and Mental Health Services Administration’s (SAMHSA’s) Division of Prevention, Traumatic Stress and Special

Programs of the Center for Mental Health Services (CMHS) has contracted with ICF Macro to conduct the cross-site evaluation.

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

☐ Yes
☒ No

22a. Identify the Privacy Act System of Records Notice (SORN) Name and Number or identify if a SORN is in progress.

Published:
Published:
Published:
In Progress

23. Identify the sources of PII in the system.

☒ Directly from and 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 No. 0930-0286
- Expiration Date: December 2013

24. Is the PII shared with other organizations?

☐ Yes
☒ No

24a. Identify with whom the PII is shared or disclosed and for what purpose.
N/A – Information is not shared with other organizations.

Are the project officers:
☐ Within HHS
☐ Other Federal
☐ Agency/Agencies
☐ 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)).
N/A

24c. Describe the procedures for accounting for disclosures
N/A

25. Describe how individuals are provided notice prior to the collection of PII. If notice is not provided, explain why not.

Research subjects, Grantees and SPDC users are notified of the use of their data and the security procedures used to ensure confidentiality during the informed consent process. Research subjects are also informed that they can drop out of the study at any time without consequence.

26 Is the submission of PII by individuals voluntary or mandatory?
☒ Voluntary
☐ Mandatory

27. Describe the method for individuals to object to the collection or use of their PII or describe why individuals cannot object.

Research subjects are provided with the contact information of the center's IRB during the informed consent process and are encouraged to inform the IRB of any misuse of PII. System users can contact ICF if they feel that any information, including their own PII, has been inappropriately obtained, misused, or inappropriately disclosed.

For access to the SPDC, grantee users are required to provide their name and email address to gain access to the system, additional contact information is optional.

Participation in the SMSS listserv is optional; students approached for their contact information are free to decline participation.

The CP is a brief survey that asks GLS grantees for contact information for organizations that participate in a coalition related to their suicide prevention grant. This

contact information is used to contact members of the organization if they are willing to participate in an online survey. The CP is a requirement of the cross-site evaluation for grantees who have reported working with a coalition as part of their grant program.

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.

The SPDC has not gone through any major system changes that would compromise or affect disclosure or data uses.

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.

Research subjects are provided with the contact information of the center's IRB during the informed consent process and are encouraged to inform the IRB of any misuse of PII. System users can contact ICF if they feel that any information, including their own PII, has been inappropriately obtained, misused, or inappropriately disclosed.

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.

ICF maintains the integrity of the data exactly as received through the SPDC. All data are validated when posted to the centralized database. There are immediate validations to identify data input errors by the user. These error messages are presented to the user for review before any data can be submitted to the system. In addition, there are database level validations to ensure that key data and any other data that are required to maintain database integrity are valid. Upon submission, the linkage between a respondent's contact information and their submitted data is broken so that analysts cannot see this linkage in data files obtained from the SPDC. ICF periodically reviews contact information in the SPDC database to ensure the information is still necessary and relevant for achieving program objectives.

31. Identify who will have access to the PII in the system and the reason why they require access.

☐ Users
☒ Administrators
☐ Developers
☒ Contractors
☐ Others

The SPDC administrator and ICF project staff (contractors) will have access to the data gathered for the CP and SMSS so that they can send surveys to potential respondents. Only the SPDC administrator has access to the SPDC user's contact information, as this information is not used and is stored on the SPDC server.

32. Describe the procedures in place to determine which users may access PII

The SPDC Administrator has access to all data on the SPDC system. Other team members do not have direct access to these data. The Administrator will provide access to information gathered via the CP and SMSS to the data collection leads for sending out survey invitations only as necessary.

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 system has multiple resource objects, including servers, databases, applications, and file directories, and access is limited to authorized project team members and network support staff. Access to data files, processing capability, software, and hardware is restricted to the minimum necessary to perform the job. Critical functions are divided among different individuals to reduce the likelihood of fraudulent activity. Specifically, The SPDC Administrator will develop a data download for the CP and SMSS leads that only include elements necessary to send surveys to potential respondents – for the CP this would include organization name and email address, for the SMSS it would include college/university name and phone number.

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.

ICF is committed to ensuring that staff members are trained in the ethical standards of confidentiality and data security when working with sensitive data. We maintain a security and confidentiality policy composed of several components, including a confidentiality and data security agreement, which is required of all ICF employees working with data; related training on confidentiality and data security protocols; an institutional review board (IRB); training for employees regarding the purposes and requirements of the IRB; and ethical guidelines prescribed by professional associations. Our security policies and procedures are reviewed at least annually and whenever new technologies are incorporated into data collection and reporting systems.

New employees are required to sign a corporate confidentiality agreement. In addition, some projects with highly confidential data have project confidentiality agreements. The human resources manager enforces the corporate confidentiality agreement. Project management enforces any special assurances that are needed for particular projects.

35. Describe training system users receive (above and beyond general security and privacy awareness training).

In addition to annual confidentiality and security awareness training, ICF staff participated in an Institutional Review Board (IRB) training which provided additional information about protecting human subjects.

36. Do contracts include 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.

SPDC data in machine-readable form are stored on a secure server and data in hardcopy form are stored in locked cabinets. When computer files containing partial or complete data submissions or statistics about individual data submissions are no longer needed, they are either securely archived or destroyed. For those files and reports kept at ICF, printed copies of data are shredded when no longer needed. A crosscut shredder is used to dispose of all printed materials, such as reports containing complete or partial records from data submissions and material that could be indirectly identifying. The Security Officer for Data Access and Processing is responsible for oversight of all printed materials and their eventual destruction.

Server disks containing SPDC data must be overwritten or degaussed before being released for other uses. Media (e.g., backup storage tapes, floppy disks, CD-ROMs) containing data must be destroyed when no longer needed. The Security Officer for Data Access and Processing, in coordination with the Security Officer for LAN and WAN Security, is responsible for oversight of all computer servers, media, and backup tapes used to store data, as well as their eventual destruction or degaussing.

Workstations may not be used to store SPDC data, and workstations are periodically checked to confirm that no data files are stored there. Any files that are found are moved to the secure project server, and the files are overwritten. A log of this activity is also maintained.

38. Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.

ICF follows all data security guidance provided by SAMHSA and implements security controls in line with National Institute of Standards and Technology (NIST) recommendations. All ICF personnel complete training on confidentially and data security. There are several levels of security and privacy features built into the SPDC.

First, all data entered into SPDC are stored in the central database server that is protected using the server's security systems. No application or user can access the survey data without an authorized database user ID and password. A designated local SPDC site administrator (one per site), registers center-approved users in the Contact Database creates each user ID and password. The Contact Database registers users in the SPDC. The database software ensures that user IDs are unique and that user information is properly registered. Users can change their passwords after their initial login using the assigned user ID and password and will be forced to change their passwords. SPDC will utilize https to provide encryption and a secure channel for all data entry and transmissions. Only the login page of the site will be publicly available and access will be limited to authorized participants with distinct usernames and passwords. A randomly generated session ID is established and passed through the system when a user logs in. Therefore, a valid session ID must exist in order for a user to access each page in the system. Sessions expire after 20 minutes of inactivity, at which time the user will be returned to the login page where the user ID and password must be reentered. For survey respondents, unique usernames and passwords are created by the SPDC administrator for each survey. These logins are disabled either after survey submission or when the administration window closes.

ICF has a process in place to monitor and respond to privacy and/or security incidents. Security concerns include security breaches and results of security reviews or audits; security status includes implementation of security safeguards and preparation of security plans. The ICF Technical Officer oversees security reporting. ICF's technical staff, including the ICF Security Officer for Data Access and Processing, meets regularly to discuss SPDC development and maintenance; security concerns and status are discussed at these meetings as needed. In addition, ICF's network support staff have periodic status meetings led by the ICF Security Officer for LAN and WAN security at which security concerns and status are discussed as needed and communicated to the SPDC Security Officer for Data Access and Processing. Security issues discussed at either of these meetings are communicated to the ICF Technical Officer. Any security breaches would be communicated to the HHS/SAMHSA/CMHS/ GPO.

39. Identify the publicly-available URL:
https://www.suicideprevention-datacenter.com

40. Does the website have a posted privacy policy?
☒ Yes
☐ No

40a Is the privacy policy available in a machine-readable format?
☒ Yes
☐ No

41. Does the website employ website measurement and customization technologies (e.g., cookies or beacons)?

☒ 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 beacon	☐ Yes ☒ No
Web bugs	☐ Yes ☒ No
Session Cookies	☒ Yes ☐ No
Persistent Cookies	☐ Yes ☒ No

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

☐ Yes
☒ No

42a. Is there a unique privacy policy for the website, and does the unique privacy policy address the process for obtaining parental consent if any information is collected?

☐ Yes
☒ No

43. Does the website contain links to websites external to HHS?

☒ Yes
☐ No

43a. Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?

☐ Yes
☒ No