Attachment 18: SAMPLE COPY HHS PRIVACY IMPACT ASSESSMENT
Web-based Skills Training for SBIRT (Screening Brief Intervention and Referral to Treatment)
November 2011

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?

If this is an existing PIA, please provide a reason for revision:

*1. Date of this Submission:

*2. OPDIV Name:

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

*5. OMB Information Collection Approval Number:

*6. Other Identifying Number(s):

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

*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	

*10. Provide an overview of the system:

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

*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?

Note: This question seeks to identify any, and all, personal information associated with the system. This includes any PII, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. If the information contained in the system ONLY represents federal contact data (i.e., federal contact name, federal address, federal phone number, and federal email address), it does not qualify as PII, according to the E-Government Act of 2002, and the response to Q.17 should be No (only the PIA Summary is required). If the system contains a mixture of federal contact information and other types of PII, the response to Q.17 should be Yes (full PIA is required).

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.

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

*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)

*23. If the system shares or discloses PII, please specify with whom and for what purpose(s):

*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:

*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.]):

*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)

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

*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)
*54. Briefly describe in detail how the PII will be secured on the system using administrative, technical, and physical controls:

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?

If this is an existing PIA, please provide a reason for revision:

*1. Date of this Submission:

*2. OPDIV Name:

3. Unique Project Identifier (UPI) Number for current fiscal year (Data is auto-populated from the System Inventory form, UPI table):

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

*5. OMB Information Collection Approval Number:

5a. OMB Collection Approval Number Expiration Date:

*6. Other Identifying Number(s):

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

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

System Location:	
OPDIV or contractor office building	
Room	

City	
State	

*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	

The following information will not be made publicly available:

POC Title	
POC Organization	
POC Phone	
POC Email	

*10. Provide an overview of the system: (Note: The System Inventory form can provide additional information for child dependencies if the system is a GSS)

SYSTEM CHARACTERIZATION AND DATA CATEGORIZATION

1 System Characterization and Data Configuration

11. Does HHS own the system?

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)

12a. If no, identify the system operator:

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

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

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	
Anonymous to Non-Anonymous	
Significant System Management Changes	
Significant Merging	
New Public Access	
Commercial Sources	
New Interagency Uses	
Internal Flow or Collection	
Alteration in Character of Data	

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

Note: This question seeks to identify any, and all, personal information associated with the system. This includes any PII, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. If the information contained in the system ONLY represents business contact data (i.e., business contact name, business address, business phone number, and business email address), it does not qualify as PII, according to the E-Government Act of 2002, and the response to Q.17 should be No (only the PIA Summary is required). If the system contains a mixture of business contact information and other types of PII, the response to Q.17 should be Yes (full PIA is required).

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)	
Date of Birth	
Social Security Number (SSN)	
Photographic Identifiers	
Driver's License	
Biometric Identifiers	
Mother's Maiden Name	
Vehicle Identifiers	
Personal Mailing Address	
Personal Phone Numbers	
Medical Records Numbers	
Medical Notes	
Financial Account Information	
Certificates	
Legal Documents	
Device Identifiers	
Web Uniform Resource Locator(s) (URL)	
Personal Email Address	
Education Records	
Military Status	
Employment Status	
Foreign Activities	
Other	

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.

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	
Public Citizen	
Patients	
Business partners/contacts (Federal, state, local agencies)	
Vendors/Suppliers/Contractors	
Other	

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

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)	
Date of Birth	
SSN	
Photographic Identifiers	
Driver’s License	
Biometric Identifiers	
Mother’s Maiden Name	
Vehicle Identifiers	
Personal Mailing Address	
Personal Phone Numbers	
Medical Records Numbers	
Medical Notes	
Financial Account Information	
Certificates	
Legal Documents	
Device Identifiers	
Web URLs	
Personal Email Address	
Education Records	
Military Status	

Employment Status	
Foreign Activities	
Other	

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

*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)

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?

Please indicate "Yes" or "No" for each category below:	Yes/No
Name (for purposes other than contacting federal employees)	
Date of Birth	
SSN	
Photographic Identifiers	
Driver's License	
Biometric Identifiers	
Mother's Maiden Name	
Vehicle Identifiers	
Personal Mailing Address	
Personal Phone Numbers	
Medical Records Numbers	
Medical Notes	
Financial Account Information	
Certificates	
Legal Documents	
Device Identifiers	
Web URLs	
Personal Email Address	
Education Records	
Military Status	
Employment Status	
Foreign Activities	
Other	

*23. If the system shares or discloses PII please specify with whom and for what purpose(s):

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?

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)?

26. Are individuals notified how their PII is going to be used?

26a. If yes, please describe the process for allowing individuals to have a choice. If no, please provide an explanation.

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?

27a. If yes, please describe briefly the notification process. If no, please provide an explanation.

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?

28a. If yes, please describe briefly the review process. If no, please provide an explanation.

29. Are there rules of conduct in place for access to PII on the system?

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		
Administrators		
Developers		
Contractors		
Other		

*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:

*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.])

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)

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		
Intranet		
Both		

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.).

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?

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)?

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

36. Does the website employ tracking technologies?

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

Other	

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

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?

Please indicate “Yes” or “No” for each category below:	Yes/No
Name (for purposes other than contacting federal employees)	
Date of Birth	
SSN	
Photographic Identifiers	
Driver's License	
Biometric Identifiers	
Mother's Maiden Name	
Vehicle Identifiers	
Personal Mailing Address	
Personal Phone Numbers	
Medical Records Numbers	
Medical Notes	
Financial Account Information	
Certificates	
Legal Documents	
Device Identifiers	
Web URLs	
Personal Email Address	
Education Records	
Military Status	
Employment Status	
Foreign Activities	
Other	

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

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

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)?

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):

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?

43. Is there a contingency (or backup) plan for the system?

44. Are files backed up regularly?

45. Are backup files stored offsite?

46. Are there user manuals for the system?

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?

48. If contractors operate or use the system, do the contracts include clauses ensuring adherence to privacy provisions and practices?

49. Are methods in place to ensure least privilege (i.e., “need to know” and accountability)?

49a. If yes, please specify method(s):

*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):

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

TECHNICAL CONTROLS

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?

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

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

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

PHYSICAL ACCESS

1	Physical Access

53. Are physical access controls in place?

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

*54. Briefly describe in detail how the PII will be secured on the system using administrative, technical, and physical controls:

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:	

PIA % COMPLETE

1	PIA Completion
PIA Percentage Complete:	
PIA Missing Fields:	