Office of the Chief Information Officer
Office of the Assistant Secretary for Administration
Department of Health and Human Services

Privacy Impact Assessment (PIA) and Privacy Threshold Analysis (PTA) Writers' Handbook

Version 2.0
April 2016

Produced by:
HHS Enterprise Privacy Program, Office of Information Security
PrivacyProgramMailbox@hhs.gov

VERSION HISTORY

Version #	Implemented By	Revision Date	Approved By	Approval Date	Reason
0.1	HHS Enterprise Privacy Program	04/17/2015			PTA/PIA Writers' Handbook for stakeholder review and feedback
0.2	HHS Enterprise Privacy Program	05/29/2015			Sent to Matt Olsen and Bridget Guenther for their review
1.0	HHS Enterprise Privacy Program	06/17/2015			Sent to Matt Olsen and Bridget Guenther for review prior to submission for leadership review/approval
2.0	HHS Privacy Program	4/20/2016			Revised to reflect updated PIA Guidance, Approved 4/20/16

Table of Contents

Introduction 1

Completing the HHS PIA Template 3

How to Use This Handbook 6

Question-By-Question Guidance 8

Q1) OPDIV 8

Q2) PIA Unique Identifier 8

Q2a) Name 9

Q3) The subject of this PIA is which of the following? 11

Q3a) Identify the Enterprise Performance Lifecycle Phase of the system 11

Q3b) Is this a FISMA-Reportable system? 12

Q4) Does the system include a Website or online application available to and for the use of the general public? 13

Q5) Identify the operator 14

Q6) Point Of Contact (POC): 14

Q7) Is this a new or existing system? 14

Q8) Does the system have Security Authorization (SA)? 15

Q8a) Date of Authorization 15

Q8b) Planned Data of Authorization 15

Q9) Indicate the following reason(s) for updating this PIA. Choose from the following options 16

Q10) Describe in further detail any changes to the system that have occurred since the last PIA. 17

Q11) Describe the purpose of the system 17

Q12) 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.) 18

Q13) Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily. 18

Q14) Does the system collect, maintain, use, or share PII? 19

Q15) Indicate the type of PII that the system will collect or maintain 20

Q16) Indicate the categories of individuals about whom PII is collected, maintained, or shared. 21

Q17) How many individuals' PII is in the system? 22

Q18) For what primary purpose is the PII used? 23

Q19) Describe the secondary uses for which the PII will be used (e.g. testing, training or research) 23

Q20) Describe the function of the SSN. …… 24

Q20a) Cite the legal authority to use the SSN.…….... 25

Q21) Identify legal authorities governing information use and disclosure specific to the system and program. …… 26

Q22) Are records in the system retrieved by one or more PII data elements?..... 29

Q22a) 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…… 30

Q23) Identify the sources of PII in the system……... 31

Q23a) Identify the OMB information collection approval number and expiration date…….. 32

Q24) Is the PII shared with other organizations?..... 33

Q24a) Identify with whom the PII is shared or disclosed and for what purpose…….... 34

Q24b) 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))……... 35

Q24c) Describe the procedures for accounting for disclosures…….. 36

Q25) Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason…… 37

Q26) Is the submission of PII by individuals voluntary or mandatory?..... 39

Q27) 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…… 40

Q28) 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…. 41

Q29) 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…… 43

Q30) 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…….. 44

Q31) Identify who will have access to the PII in the system and the reason why they require access…….. 46

Q32) Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII……... 47

Q33) 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……. 47

Q34) 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…… 48

Q35) Describe training system users receive (above and beyond general security and privacy awareness training)…… 49

Q36) Do contracts include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices?..... 50

Q37) Describe the process and guidelines in place with regard to the retention and destruction of PII. Cite specific records retention schedules…….. 51

Q38) Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls…….. 53

Q39) Identify the publicly-available URL:..... 54

Q40) Does the website have a posted privacy notice?..... 55

Q40a) Is the privacy policy available in a machine-readable format?..... 56

Q41) Does the Website use web measurement and customization technology?..... 57

Q41a) Select the type of website measurement and customization technologies is in use and if it is used to collect PII. (Select all that apply)……..…… 58

Q42) Does the website have any information or pages directed at children under the age of thirteen?..... 59

Q42a) 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?..... 60

Q43) Does the website contain links to non-federal government websites external to HHS?..... 60

Q43a) Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?..... 61

Appendix I: SORNs And PIAs…….…… 62

Appendix II: Legal Authorities……..... 64

Appendix III: Useful Acronyms……..…. 66

Appendix IV: Useful Terminology……..... 68

Appendix V: Included Authorities Organized By Topic……... 74

Introduction[1]

The E-Government Act of 2002 Section 208 (E-Government Act) and Office of Management and Budget (OMB) Memorandum M-03-22, Guidance for Implementing the Privacy Provisions of the E-Government of 2002, form the core of the Privacy Impact Assessment (PIA) requirement. Together, they state that a PIA is an assessment of how information is handled within certain electronic systems. Each PIA should consider:

- Whether the system complies with legal, regulatory, and policy requirements related to privacy;
- The risks and effects of how that system handles personally identifiable information (PII); and
- How the system could be changed to mitigate potential privacy risks.

The E-Government Act and M-03-22 also state that federal agencies are required to complete PIAs for certain electronic systems, have those PIAs approved by the agency's Chief Information Officer (CIO) or a delegate thereof, and then make each PIA publically available when practical.

The Department of Health and Human Service (HHS) has chosen to evaluate the privacy implications of all electronic systems regardless of whether the E-Government Act or OMB M-03-22 requires a PIA. Each evaluation is completed via the same electronic form called the PIA/PTA Template and signed by a delegate of the CIO. Currently, the two major differences are that:

- Evaluations required by the aforementioned laws are called PIAs while those required by HHS policy are called Privacy Threshold Analysis (PTAs);[2] and
- All PIAs are published on HHS's website while PTAs may not be published.

This Handbook is designed to help authors and reviewers complete the PIA/PTA Template questions. It provides guidance on what should be included in each answer and some of the key

[1] Some of the authorities which are relevant to this introduction include:
- The Privacy Act of 1974, as amended;
- OMB Memorandum M-05-08, Designation of Senior Agency Officials for Privacy;
- HHS-OCIO-2009-0002.001, HHS OCIO Policy for Privacy Impact Assessment (PIA), Section 5.1.1;
- HHS-OCIO-2011-0003, Revisions to the HHS-OCIO Policy for Information Systems Security and Privacy, Sections 5.8.18 and 5.9;
- HHS-OCIO-2013-0002, HHS Information Sharing Environment (ISE) Privacy Policy; and
- HHS Memo for Change of Review Period for Privacy Impact Assessments (on intranet).

[2] The name PTA is used for this document because part of the analysis that goes into completing a PTA is also used to determine whether a PIA is required.

authorities that lead to the inclusion of each question.[3] If you think advice in this walkthrough contradicts guidance provided by your Operating Division (OpDiv), please contact your OpDiv's Senior Official for Privacy (SOP) for clarification.

Beyond the guidance provided in this walkthrough, and any guidance provided by your OpDiv, your PIA may include whatever additional information is needed to fully describe a system and its privacy implications.

[3] Any text underlined with dots, as in this sentence, is a hyperlink to additional content located on a federal website. Since these websites are not maintained by the HHS Enterprise Privacy Program, we cannot guarantee that the content or link will remain the same.

Completing the HHS PIA Template

Before starting to fill out the HHS PIA Template, we recommend obtaining and reviewing any available program and system documentation. This may include:

- Websites which explain the service or business process supported by the system;
- Information Collection Requests (ICRs) if the system collects information from the public and is subject to the Paperwork Reduction Act (PRA);
- Privacy Act Statements (PASs) and System of Records Notices (SORNs) if records in the system are subject to the Privacy Act;
- Agency IT Portfolio Summaries (formerly called Exhibit 53s) or any Major IT Investment Business Cases (formerly called Exhibit 300s);
- Enterprise Program Lifecycle Artifacts such as a System Security Plan (SSP); and
- Any handbooks or other guidance on how to use the system.

It may be possible to reuse language from these documents to respond to questions. However, make sure you review all copied text to verify that it is specific to the system being reviewed, is complete, and makes sense absent the rest of the document. Text copied from marketing materials and system planning documents may discuss functions that were never purchased or implemented. Text copied from a SORN or budget document may describe more than one system.

It is important to remember that the completed PIA/PTA Template may be published on HHS's website where it will be available to the general public. For this reason, it should be written so that someone with no system knowledge, and limited IT knowledge, could understand its purpose and what information it collects, maintains, and shares.

- **Limit the use of jargon and technical terms to the greatest extent possible.**
- **Define all acronyms, terms of art, jargon, and/or technical terms at first use.**
    - Define and describe:
        - Acronyms other than HHS, IT, PIA, PTA, and OpDiv names;
        - Names of computer programs which are not typically found on a home computer; and
        - Names of HHS programs and services except for those which are as well-known as Healthcare.gov or Medicare.
    - Do not define an acronym, term of art, or technical term more than once in the document.
    - If a system name contains an undefined acronym or term of art, you should:
        - Define the system name the first time it is written in a text box; and

- Consider working with your HHS Enterprise Architecture Repository (HEAR) representative to change the system name in HEAR to include the commonly used acronym.[4]

- **Responses in text boxes should include lists and/or be written in complete sentences with proper grammar and formatting.**
  - Maintain a consistent format throughout a list (do not change the style of bullets halfway through).
  - Use spell check.
  - Review the PIA/PTA Template for grammatical mistakes.
  - Ensure all entries in open text boxes are written in complete sentences.

- **Use clear and concise language.**
  - Descriptions should be written in plain and easily understood language.
  - Descriptions should be as specific as possible.
    - Financial information is an example of a vague description because it could comprise a multitude of information including credit card number and name, purchasing history, bank routing numbers, social security numbers (SSNs), names and addresses, et cetera.
    - Demographic information is another example of a vague description because it could comprise a multitude of information including race, national origin, ethnicity, economic situation, age, gender, et cetera.

- **Only use the word mandatory in accordance with the Privacy Act definition.[5]**
  - Mandatory: Failure to provide the requested information may lead to a civil or criminal penalty.
  - Voluntary: Failure to provide the requested information may lead to any other negative repercussions.
    - NOTE: If an individual voluntarily provides information in order to obtain a benefit or privilege, the government's request for information to process that benefit or privilege will be voluntary.

[4] HEAR is an inventory system used to track several information systems within HHS.

[5] OMB Privacy Act Implementation: Guidelines and Responsibilities, 40 FR 28962 includes an explanation of the differences between mandatory and voluntary.

- **Do not provide sensitive or confidential information that could allow unauthorized system access or harm. Examples include (but are not limited to) the following:**
  - Listing very detailed information about a system's security controls.
  - Stating how often a security guard patrols a building containing a server.
- **Do not include PII in a response except when responding to Question 6.**
  - Question 6 requests information about the system's point of contact and will not be published online.
  - Responses to all other questions may be published online so they should not contain PII.
- **All questions should be answered unless this Handbook states otherwise.**
  - Unless stated in this Handbook, the HHS Security Data Warehouse (HSDW) may automatically send a draft PIA with an unanswered question back to the draft or re-draft queue for further revisions.
- **Limit the PIA to current system activities.**
  - All PIAs should be written in present tense. A PIA/PTA Template for a:
    - Yet-to-be-deployed system should describe the system on day one of its full deployment/use (i.e., the first day that it goes live).
    - System undergoing a triennial review should describe the system at the time of the review.
    - System undergoing changes that create one or more new privacy risks (see Question 9) should describe the system with those changes.
  - When writing a PIA for a replacement or updated system, avoid discussing how the replacement or updated system differs from the prior system because the general public may not know enough about the prior system to understand the comparison.
- **Completing a PIA may require collaboration between several individuals including:**
  - Your OpDiv's HEAR representative;
  - Your OpDiv's FISMA System Inventory representative;
  - Your OpDiv's Records or Information officer;
  - Your OpDiv's Senior Official for Privacy;
  - Your OpDiv's Office of General Council; and
    - The Departmental Privacy Act Officer in the Office of the Assistant Secretary for Public Affairs (OS/ASPA).

How to use this Handbook

This Handbook contains advice on Questions 1 through Question 43 and includes all subparts. It does not discuss the twelve (12) Reviewer Questions; those questions and answers are not published and may be used however your OpDiv's SOP chooses. For almost each question or subpart, there is a table which provides a standard set of information. In a few situations, closely interrelated questions and/or subparts are covered together in one table.

Some of the answers in the PIA/PTA Template have a gray background because they are automatically populated and cannot be changed via the form. The information used to auto-populate these questions comes from three sources:

- The form in HSDW that was used to create the PIA/PTA Template;
- HEAR; and
- The FISMA System Inventory.

One of the questions asked when creating a new PIA/PTA Template is whether the system is assigned a System Universal Unique Identifier (UUID). Generally speaking:

- If nothing is provided in that box, HSDW will fill the gray questions with information provided when the PIA/PTA Template was originally created or provide a default answer.
- If a System UUID is provided which matches HEAR and/or the FISMA System Inventory, the gray questions will be updated to match HEAR and/or the FISMA System Inventory whenever the PIA/PTA Template is downloaded or uploaded.
- If a System UUID is provided which does not match HEAR and/or the FISMA System Inventory, the gray questions may show no answer or a strange answer.

For these questions, the table will contain one or more of the following sections:

The Question	
Auto-populated response:	• *The logic used to auto-populate this response.*
To address any issues:	• *How to change an auto-populated response.*
Key terms:	• *Definitions of terms which are key or specific to this question.*
Authorities and guidance:	• *Some of the authorities that lead to the inclusion of this question and, in some situations, a summary of what that authority includes.* • *Non-binding guidance that may help explain this question.*
Skip logic:	• *If an answer to an earlier question will cause this question to disappear.* • *If an answer to this question will cause a later question to disappear.*

If a question has no gray background, which indicates that it may be completed by a PIA writer, the table will contain one or more of the following sections:

The Question	
How to approach the question:	• *The information that should be included in the response. As noted above, you may include additional information when feasible in order to further explain the system.*
Additional considerations:	• *Advice, tips, and/or a further explanation of what information could or should be included in this section.*
Key terms:	• *Definitions of terms which are key or specific to this question.*
Authorities and guidance:	• *Some of the authorities that lead to the inclusion of this question and, in some situations, a summary of what that authority includes.* • *Non-binding guidance that may help explain this question.*
Skip logic:	• *If an answer to an earlier question will cause this question to disappear.* • *If an answer to this question will cause a later question to disappear.*

The HHS PIA Template automatically reveals and hides questions based on responses to preceding questions. For example, stating that a system does not include a website for use of the general public will hide later questions about the system's website. For this reason, we recommend completing the questions in the order asked.

Question-by-Question Guidance

Q1) OpDiv	
Auto-populated response:	• This should display the OpDiv of the individual who created the PIA at the time the PIA was created.
To address any issues:	• If a downloaded PIA displays the wrong OpDiv, send an e-mail to PrivacyProgramMailbox@hhs.gov which includes: o The name of the PIA; o The PIA Unique Identifier; o The currently listed OpDiv; o What OpDiv should be listed; and o Whether you just created this PIA or if this PIA was already in HSDW. • The HHS Privacy Program will work with HSDW and communicate with you to fix the error. In many situations, the HSDW Developers will change information in HSDW to reflect the correct OpDiv. Once that is done, you will be able to download a new PDF which will show the correct OpDiv. The PDF with the incorrect OpDiv can no longer be uploaded into HSDW. If that is the solution, we recommend copying all responses from the old PDF to the new PDF and then deleting the old PDF.

Q2) PIA Unique Identifier	
Auto-populated response:	• This should display an HSDW-generated number.
To address any issues:	• This number should not affect the PIA review so it should not need to change.

Q2a) Name	
Auto-populated response:	• The form in HSDW which is used to create a new PIA/PTA Template requests a System UUID. When you first create a PIA and return to the New Draft queue, you will see a listing with the name you provided on the form used to create the PIA. If you download a PIA and the System UUID was: o Left blank on the creation form, the downloaded PIA will display the name entered at creation. o Not left blank on the creation form, HSDW will replace the name you provided at creation with the name linked to that System UUID in HEAR. ▪ If the System UUID provided on the creation form does not match a System UUID listed in HEAR, the PIA/PTA Template name will be blank. • When you download a PIA for updates: o If the System UUID is blank, the downloaded PIA should display the name entered into HSDW when it was originally created. o If a System UUID is not blank, the downloaded PIA should display the name associated with that System UUID in HEAR. ▪ If the name in HEAR is changed, the PIA should display the new name when it is downloaded. ▪ If the System UUID is not found in HEAR, the PIA name should be blank.

Q2a) Name	
To address any issues:	• If a UUID is provided when a new PIA is created in HSDW, the provided name will be replaced with whatever is linked to that UUID in HEAR when it is first downloaded. If no UUID is provided, we recommend giving the PIA a name that: o Matches other documentation about that system; and o Defines any acronyms used in the name. • Check the PIA's listing in HSDW to see if a System UUID is listed. o If no System UUID is listed, send an email to PrivacyProgramMailbox@hhs.gov which includes the current name of the PIA, the PIA Unique Identifier, and what the name should be. o If a System UUID is listed, the System UUID and/or system name may not be properly listed in HEAR. This can be fixed by following these steps (in order): ▪ Ask your HEAR representative to verify that HEAR includes the correct System UUID and system name. ▪ Confirm that your HEAR representative made any necessary updates. ▪ Send an e-mail to PrivacyProgramMailbox@hhs.gov which includes the current name of the PIA, the PIA Unique Identifier, and what the name should be. ▪ Wait for a response from PrivacyProgramMailbox@hhs.gov and then follow the steps in that response. • In many situations, the HSDW Developers will fix the issue by changing information in HSDW. Once that is done, you will be able to download a new PDF which will show the correct name. The PDF with the incorrect name can no longer be uploaded into HSDW. If that is the solution, we recommend copying all responses from the old PDF to the new PDF and then deleting the old PDF.

Q3) The subject of this PIA is which of the following?	
How to approach the question:	• Select the appropriate radio button.
Additional considerations:	• Any questions about Q3 should be directed to your OpDiv's FISMA System Inventory representative.
Authorities and guidance:	• OMB Circular No. A-130 Revised Appendix III. • NIST Special Publication 800-100, Information Security Handbook: A Guide for Managers, Section 8.1, Major Applications, General Support Systems, and Minor Applications. • HHS Standard 2008-0006.001S, HHS Standard for FISMA Inventory Management.

Q3a) Identify the Enterprise Performance Lifecycle phase of the system.	
How to approach the question:	• Select the phase of the HHS Enterprise Performance Lifecycle (EPLC) Framework that best matches the phase of the system.
Key terms:	• Enterprise Performance Lifecycle (EPLC) Framework: An HHS framework to enhance Information Technology (IT) governance through rigorous application of sound investment and project management principles and industry's best practices. The HHS EPLC provides the context for the HHS IT governance process and describes interdependencies between its project management, investment management, and capital planning components. The phases are defined in HHS' Enterprise Performance Life Cycle Framework Overview Document.

Q3b) Is this a FISMA-Reportable system?	
Auto-populated response:	• This answer should be yes if the System UUID associated with this PIA matches a listing in your OpDiv's FISMA System Inventory. • This answer should be no if: o No System UUID is associated with this PIA; or o The System UUID does not match a listing in your OpDiv's FISMA System Inventory.
To address any issues:	• If a PIA for a FISMA-Reportable system incorrectly states that the system is not FISMA-Reportable, this can be fixed by following these steps (in order): o Ask your OpDiv's FISMA System Inventory representative to verify that the FISMA System Inventory includes the correct System UUID. o Confirm that your OpDiv's FISMA System Inventory representative made any necessary updates. o Send an e-mail to PrivacyProgramMailbox@hhs.gov which includes the name of the PIA, the PIA Unique Identifier, the current status, and what the status should be. o Wait for a response from PrivacyProgramMailbox@hhs.gov and then follow the steps in that response. • In many situations, the HSDW Developers will fix the issue by changing information in HSDW. Once that is done, you will be able to download a new PDF which will show the correct status. The PDF with the incorrect status can no longer be uploaded into HSDW. If that is the solution, we recommend copying all responses from the old PDF to the new PDF and then deleting the old PDF.
Authorities and guidance:	• 44 USC 3505(c): A requirement to maintain a system inventory. • HHS Standard 2008-0006.001S, HHS Standard for FISMA Inventory Management.

Q4) Does the system include a Website or online application available to and for the use of the general public?	
How to approach the question:	• If the system includes one or more websites, the response should generally be yes unless all websites are only used for: o Internal agency activities (such as on intranets, internal applications, or interactions that only involve HHS employees and/or contractors directly supporting HHS); and/or o Activities that involve authorized law enforcement, national security, or national intelligence.
Additional considerations:	• If members of the public can view a login page, but only employees and/or contractors directly supporting HHS receive login credentials, the answer should be no. • Websites which collect information for use in a system are generally considered part of the system. Conversely, HHS.gov webpages that describe a particular system, such as this webpage about the Adoption Assistance Program, are not generally considered part of the system. The Office of the Secretary and OpDivs have written separate PIAs and PTAs that evaluate the privacy implications of these websites.
Authorities and guidance:	• OMB M-03-22 Attachment A, Section III, Privacy Policies on Agency Websites: Guidance on the need to have a privacy policy when a federal agency operates a website which is available to the public. • OMB M-10-22 Attachment 1: Guidance on the use of web measurement and customization technologies when a federal agency operates a website.
Skip logic:	• If Q4 is no, Q39 through Q43a should no longer appear on the form.

Q5) Identify the operator.	
Auto-populated response:	• This answer will be auto-populated based on the FISMA System Inventory.
To address any issues:	• If a PIA for a FISMA-Reportable system incorrectly identifies the system's operator, this can be fixed by following these steps (in order): o Ask your OpDiv's FISMA System Inventory representative to verify that the FISMA System Inventory includes the correct System UUID and status. o Confirm that your OpDiv's FISMA System Inventory representative made any necessary updates. o Send an e-mail to PrivacyProgramMailbox@hhs.gov which includes the name of the PIA, the PIA Unique Identifier, the current status and what the status should be. o Wait for a response from PrivacyProgramMailbox@hhs.gov and then follow the steps in that response. • In many situations, the HSDW Developers will fix the issue by changing information in HSDW. Once that is done, you will be able to download a new PDF which will show the correct status. The PDF with the incorrect status can no longer be uploaded into HSDW. If that is the solution, we recommend copying all responses from the old PDF to the new PDF and then deleting the old PDF.

Q6) Point of Contact (POC):	
How to approach the question:	• Provide the title, name, organization, e-mail, and phone number of the individual(s) who may be contacted for inquiries about the system.
Additional considerations:	• This information is used for internal purposes, but will not be published online with the rest of the PIA. • If two or more individuals and their contact information is listed, state which contact information corresponds to which individual.

Q7) Is this a new or existing system?	
Auto-populated response:	• The form should automatically select: o Existing if the PIA has been signed (i.e., finalized) at least once; or o New if the PIA has never been signed (i.e., finalized).
To address any issues:	• Send an e-mail to PrivacyProgramMailbox@hhs.gov which includes the name of the PIA, the PIA Unique Identifier, the current status, and what the status should be. • In many situations, the HSDW Developers will fix the issue by changing information in HSDW. Once that is done, you will be able to download a new PDF which will show the correct status. The PDF with the incorrect status can no longer be uploaded into HSDW. If that is the solution, we recommend copying all responses from the old PDF to the new PDF and then deleting the old PDF.
Skip logic:	• If Q7 is new, Q9 and Q10 should no longer appear on the form.

Q8) Does the system have Security Authorization (SA)? **Q8a) Date of Authorization** **Q8b) Planned Data of Authorization**	
Auto-populated response:	• If the System UUID matches a listing in the FISMA System Inventory, the PIA should display the SA date listed in the FISMA System Inventory. • If the System UUID does not match a listing in the FISMA System Inventory, the PIA should state that the system does not have a SA. • If the system requires an SA and does not have one, provide the date when the system should receive its SA. • If the system will not require a SA, select the button indicating that a SA is not applicable.
To address any issues:	• If the PIA incorrectly states that the system does not have a SA, or lists the wrong date, this can be fixed by following these steps (in order): o Ask your OpDiv's FISMA System Inventory representative to verify that the FISMA System Inventory includes the correct System UUID and SA date. o Confirm that your OpDiv's FISMA System Inventory representative made any necessary updates. o Send an e-mail to PrivacyProgramMailbox@hhs.gov which includes the name of the PIA, the PIA Unique Identifier, the current status, and what the status should be. o Wait for a response from PrivacyProgramMailbox@hhs.gov then follow the steps in that response. • In many situations, the HSDW Developers will fix the issue by changing information in HSDW. Once that is done, you will be able to download a new PDF which will show the correct status. The PDF with the incorrect status can no longer be uploaded into HSDW. If that is the solution, we recommend copying all responses from the old PDF to the new PDF and then deleting the old PDF.
Key terms:	• Security Assessment & Authorization (SA&A): A process, previously called Certification & Accreditation (C&A), which is used by HHS to evaluate the security aspects of each system. • Security Authorization (SA): Also called the Authority to Operate (ATO), this document states that the SA&A has been completed for a system and a senior HHS official will accept the risks of the system if certain security controls are implemented. SAs can be valid for as long as three years.
Authorities and guidance:	• 44 USC 3544(b): A requirement to develop, document, and implement an agency-wide information security program. • CMS Information Security Overview: A document produced by CMS which contains some general information on the SA&A process.

Q9) Indicate the following reason(s) for updating this PIA. Choose from the following options.	
How to approach the question:	• This question asks why the PIA is being updated. o If this PIA is being updated because HHS policy states that a PIA should be updated every three years, select PIA Validation (PIA Refresh/Annual Review). o If this PIA is being updated because a system change will cause one or more new privacy risks, select the applicable changes or describe the changes in the text box.
Additional considerations:	• Generally speaking, a PIA should be updated when a system change will create one or more new privacy risks. o Not all system changes will create a new privacy risk. o One system change could result in one or more new privacy risks.
Key terms:	OMB M-03-22 Attachment A provides examples of what system changes could result in a new privacy risk and therefore require an update to an existing PIA. Although the below list of terms is the same as that in M-03-22, the definitions have been revised for clarity: • Anonymous to Non-Anonymous: Anonymous information stored in a system will be changed into PII. For example, a system containing survey results, which are currently linked to an anonymous identifier, will be linked to PII. • New Public Access: A system accessed by members of the public will begin using a new user-authenticating technology (e.g., password, digital certificate, biometric identifier). • Internal Flow or Collection: New types of PII will be added to a system and/or a major change will be made to how a system uses or discloses PII already in a system. • Commercial Sources: PII purchased or obtained from commercial or public sources will be added to a system on a regular basis. Note that adding commercial or publicly acquired PII to a system on an ad hoc basis is not considered a new privacy risk. • Significant System Management Changes: The way a system manages PII will significantly change. For example, a system containing PII that is currently maintained on an HHS server will move to the cloud. • Alteration in Character of Data: New PII will be added to a system and that will cause a new privacy risk. For example, health or financial information will be added to a system that currently contains only contact information. • New Interagency Uses: A significantly new use or exchange of PII will occur because HHS will work with one or more other federal agencies to share functions. • Conversion: Records currently in paper form will be scanned or otherwise added into a system.
Authorities and guidance:	• OMB M-03-22 Attachment A: A requirement to update a PIA before a system change creates a new privacy risk and defines the key terms above. • HHS OCIO 2009-0002.001, Policy for Privacy Impact Assessment (PIA), Section 4.2, Annual Review and Major Changes. • HHS Memo for Change of Review Period for Privacy Impact Assessments (on intranet): The HHS requirement to update a PIA every three years.
Skip logic:	• Q9 should only appear if a PIA was previously completed for the system (i.e., Q7 states that this is an existing system).

Q10) Describe in further detail any changes to the system that have occurred since the last PIA.	
How to approach the question:	• Describe all system changes that have occurred since the PIA was last finalized. • Write not applicable if no changes have occurred since the PIA was last finalized.
Additional considerations:	• Q9 asks about system changes which create a new privacy risk and therefore require a PIA update. Q10 asks for a description of all changes that: o Have occurred since the PIA was last finalized; and o Will occur before the PIA is finalized. This includes a written description of what lead to the checkboxes or textboxes being completed in Q9. However, it also includes any changes that have not resulted in the need to select or answer Q9. For example, changing which contractor is responsible for a system, or changing the physical location of a server, may not affect a system's privacy risk, but should still be documented in Q10.
Authorities and guidance:	• OMB M-03-22 Attachment A, Section C: A list of what should be evaluated in a PIA and when a PIA should commence.
Skip logic:	• Q10 should only appear if a PIA was previously completed for the system (i.e., Q7 states that this is an existing system).

Q11) Describe the purpose of the system.	
How to approach the question:	• This response should describe: o What HHS functions are supported by the system; and o What the system does for each of those functions.
Additional considerations:	• This response should be: o Thorough enough that a reader with no prior knowledge of the system or what it supports will be able to understand the rest of the PIA; and o Simple enough that a reader with limit technical knowledge will be able to understand the explanation. • This response does not need to describe what PII is collected into and/or maintained in the system; several other questions in the HHS PIA Template request that information. • At least part of this response may already exist in a planning document or the website that describes the program served by the system.
Authorities and guidance:	• OMB M-03-22 Attachment A, Section C: A list of what should be evaluated in a PIA and when a PIA should commence.

Q12) 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.)	
How to approach the question:	• List and/or describe all the types of information that are collected into and/or maintained in the system regardless of: o Whether that information is PII; o How long that information is stored. • Any types of PII selected in Q15 should also be listed and/or described in Q12.
Additional considerations:	• If the system collects information (i.e. user credentials) about system users/administrators in order to control access or similar, describe the information that is collected about those users/administrators. Unless users enter a system through separate access control software, systems that require a login usually collect usernames, passwords, and/or e-mails. If user access is validated by a separate system (ex. a GSS validating a user's identity and access privileges to the system via a token or similar), and no user credentials are collected by the system covered by this PIA, include this in your response. Name the system providing access and confirm that system is covered by PIA. • If contractors use HHS credentials to access the system, label these contractors as "direct contractors" in your response. • The best response may be a list of each data element. However, groups of data elements can be summarized if the public can easily understand the summary: o Medical records can be written instead of listing out medical conditions, diagnoses, hospital stays, and the names and phone numbers of doctors since the public should generally know what information is often incorporated into a medical record. o Medicare enrollment information is too vague because the public will likely not know what information is involved in Medicare enrollment. • This response should help fulfill the OMB M-03-22 Attachment A, Section C, requirement that a PIA analyze and describe what information is to be collected.
Key terms:	• Access control software: Software that authenticates a user's credentials before they are given access to an intended system or resource, such as this example of CMS's Identity & Access Management System.
Authorities and guidance:	• OMB M-03-22 Attachment A, Section C: A list of what should be evaluated in a PIA and when a PIA should commence.

Q13) Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.	
How to approach the question:	• Describe why each type of information listed in Q12 is collected into and/or maintained in the system, or shared with another system. This description should: o Consider all information regardless of whether it is PII; o Specify what information is collected about each category of individual; and

	○ If records are routinely retrieved by PII data elements, please specify which PII data elements are used.
Additional considerations:	• This response should help fulfill the OMB M-03-22 Attachment A, Section C, requirement that a PIA analyze and describe: ○ What information is to be collected; ○ Why the information is being collected; and ○ The intended use of the information. • If contractors use HHS credentials to access the system, label these contractors as "direct contractors" in your response.
Authorities and guidance:	• OMB M-03-22 Attachment A, Section C: A list of what should be evaluated in a PIA and when a PIA should commence.

Q14) Does the system collect, maintain, use, or share PII?	
How to approach the question:	• The response should be yes if the system collects and/or maintains any PII for any length of time. ○ This includes any type of PII regardless of sensitivity. ○ This includes any system which: ▪ Acts as a conduit for PII (even if it is not maintained in the system). ▪ Collects and/or maintains PII for a short-term purpose then discards it.
Additional considerations:	• PII should be protected even if it is only maintained in the system for a short period of time. • Remember that user credentials are considered PII. • This response should help fulfill the OMB M-03-22 Attachment A, Section C, requirement that a PIA analyze and describe: ○ What information is to be collected; ○ Why the information is being collected; ○ The intended use of the information; and ○ With whom the information will be shared.
Key terms:	• Personally Identifiable Information (PII): Defined in OMB M-07-16 Footnote 1 as information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. The types of PII listed in Q15 include some of the types of PII that are commonly collected by HHS systems. Other examples may include: ○ Work information including work e-mails and work phone numbers; ○ Job titles since many people have a title that is unique to them; ○ Home phone numbers and addresses, even if they are publically available; ○ Family relationships; and ○ E-mails provided when registering for a system.
Authorities and guidance:	• OMB M-03-22 Attachment A, Section C: A list of what should be evaluated in a PIA and when a PIA should commence. • OMB M-07-16 Footnote 1: The definition of PII.
Skip logic:	• If Q14 is marked no, Q15 through Q38 should no longer appear on the form.

Q15) Indicate the type of PII that the system will collect or maintain.	
How to approach the question:	• Each element of PII collected into and/or maintained in the system should be: o Selected from the list of commonly included PII; or o Briefly described in the text boxes. • This includes every element of PII regardless of: o Type; o Sensitivity; or o Whether it is from employees or the public. • Any types of PII discussed in the rest of the PIA should also be selected and/or described in this answer.
Additional considerations:	• If the system collects information (i.e. user credentials) about system users/administrators in order to control access or similar, use the open response fields to capture that information. • This response should help fulfill the OMB M-03-22 Attachment A, Section C, requirement that a PIA analyze and describe what information is to be collected.
Authorities and guidance:	• OMB M-07-16 Footnote 1: The definition of PII.
Skip logic:	• Q15 should only appear if the system contains PII (i.e., Q14 is marked yes).

Q16) Indicate the categories of individuals about whom PII is collected, maintained, or shared.	
How to approach the question:	• Select, or describe in the text box, whose PII is collected, maintained, or shared via the system.
Additional considerations:	• This response should help fulfill the OMB M-03-22 Attachment A, Section C, requirement that a PIA analyze and describe what information is to be collected.
Key terms:	• Employees: PII is collected into and/or maintained about (1) HHS employees who are directly supporting HHS (2) because of the work those employees are doing for HHS. o Please note that direct contractors using HHS credentials are considered HHS employees for the purposes of filling out the PIA form. o Individuals applying for positions to work for HHS should be considered employees when they have received a job offer. Before that time, they should be listed as public citizens. o Employees should not be selected if a system collects from members of the general public and some of those individuals only happen to be employees. For example, select public citizens if a system collects PII about all Medicare recipients regardless of whether some may be employees. • Public citizens: Can be selected when PII is collected into and/or maintained about an individual and none of the other checkboxes apply. • Business partners/contacts (federal, state, local agencies): PII is collected into and/or maintained about individuals, such as grantees, who work with HHS or its OpDivs. • Vendors/suppliers/contractors: PII is collected into and/or maintained about individuals that provide a service to HHS. Please note that direct contractors using HHS credentials are considered HHS employees for the purposes of filling out the PIA form. • .Patients: PII is collected into and/or maintained about individuals in the context of receiving medical care.
Authorities and guidance:	• OMB M-03-22 Attachment A, Section C: A list of what should be evaluated in a PIA and when a PIA should commence.
Skip logic:	• Q16 should only appear if the system contains PII (i.e., if Q14 is marked yes).

Q17) How many individuals' PII is in the system?	
How to approach the question:	• Select the range indicating the number of individuals whose PII is maintained in the system.
Additional considerations:	• If the system collects and/or maintains PII from system users in order to control system access, the number of system users should be included in the total. • This response may be left blank if the system collects PII from individuals but that PII is not maintained in the system. This rare event generally involves a system that: o Collects PII to calculate something and then deletes it; or o Is used for internet connectivity such as a Local Area Network. • If a form used to collect information into the system includes an OMB Control Number (a Paperwork Reduction Act requirement), an ICR package should have been used to request that OMB Control Number. That ICR package should include an estimate of how many individuals are expected to complete the form. That number may help you when determining how many individuals' PII will be collected into the system.
Key terms:	• OMB Control Number: A number and expiration date that are required to be displayed on a form that collects information from members of the public if the information collection is subject to the PRA. • Information collection request (ICR): The supporting statement and attachments used to request an OMB Control Number.
Authorities and guidance:	• 44 USC 3507 i.e., The Paperwork Reduction Act of 1995: OMB Control Number requirements. • OMB M-03-22 Attachment A. • Frequently Asked Questions About PRA / Information Collection. • HHS Guidance for completing an ICR.
Skip logic:	• Q17 should only appear if the system contains PII (i.e., if Q14 is marked yes).

Q18) For what primary purpose is the PII used? Q19) Describe the secondary uses for which the PII will be used (e.g. testing, training or research)	
How to approach the question:	• Describe: o All the ways that PII is used in the system; and o When, where, and why that PII is disclosed and/or shared.
Additional considerations:	• Q18 should have a response since a system should not collect and/or maintain PII for any length of time unless it is needed for at least one primary use. However, not applicable is an appropriate response for Q19 if there is no secondary use. • If user credentials are collected, in the response to Q18, state that user credentials are collected to control system access. • If a purpose/use seems fit into both answers, you may choose whether to discuss that purpose/use in response to either Q18 or Q19. • If SORNs are applicable to the system, the purposes of the system and routine uses sections may help when responding to this question. • These responses should help fulfill the OMB M-03-22 Attachment A, Section C, requirement that a PIA analyze and describe why the information is being collected.
Key terms:	• Primary reason for collecting PII: Why a system is collecting and maintaining a particular individual's PII. For example, individual X cannot be enrolled in Medicare without submitting their PII. • Secondary reason for collecting PII: What will a system do with an individuals' PII regardless of whether that particular individual's PII is collected or maintained in the system. For example, using Medicare enrollment information to determine the average age of all Medicare enrollees does not significantly rely on individual X's enrollment.
Authorities and guidance:	• OMB M-03-22 Attachment A, Section C: A list of what should be evaluated in a PIA and when a PIA should commence.
Skip logic:	• Q18 and Q19 should only appear if the system contains PII (i.e., Q14 is marked yes).

Q20) Describe the function of the SSN.	
How to approach the question:	• If the SSN is collected into and/or maintained in the system for any length of time (as stated in Q15), use this space to describe: o All the ways that SSN is used in the system; o When, where, and why that SSN is disclosed and/or shared; and o Why the system uses the SSN instead of another identifier. • If the SSN is not collected into and/or maintained in the system, the response should be not applicable.
Additional considerations:	• This response should help fulfill the OMB M-03-22 Attachment A, Section C, requirement that a PIA analyze and describe what information is to be collected into and why the information is being collected.
Authorities and guidance:	• Public Law 93–579 Section 7 aka 5 USC § 552a (note) (page 1909): A federal agency may not deny an individual any right, benefit, or privilege provided by law because the individual refuses to provide his or her SSN unless (1) the disclosure is required by federal statute or (2) the SSN will be used to verify the individual's identity in a system of records that was operating before 1975 based on a statute or regulation adopted before 1975. It also says a federal agency that requests an individual's SSN shall inform the individual whether disclosure of the SSN is mandatory or voluntary, what legal authority requires or permits the agency to collect the SSN, and how the SSN will be used. • E.O.13478: The Executive Order that changed E.O. 9397 to no longer require the SSN to be used as a personal identifier. • OMB M-07-16 Attachment 1: Requires agencies to eliminate unnecessary use of the SSN. • OMB Letter to GAO dated 6/8/07 (copy included in GAO-07-752): Recommends the elimination of both full and truncated SSNs. • HHS Response Plan to M0716 070919: Response to Attachment 1: Safeguarding Against the Breach of Personally Identifiable Information (PII).
Skip logic:	• Q20 should only appear if the system contains PII (i.e., Q14 is marked yes).

Q20a) Cite the legal authority to use the SSN.	
How to approach the question:	• If the SSN is collected into and/or maintained in the system, as stated in Q15 and Q20, this response should: o Cite the legal authorities which permit or require the use of the SSN; and o Explain how those authorities permit the use of the SSN if not evident from the cited authorities. The cited legal authorities should include at least: o One statute or Executive Order if the collection began after 1975. o One statute, Executive Order, or regulation if the collection began before 1975. • If the SSN is not collected into and/or maintained in the system, the response should be not applicable.
Additional considerations:	• How to find the legal authorities that require or permit collection of the SSN: o Almost every system that collects the SSN will require a SORN and that SORN will almost always list the legal authorities that require or permit collection of the SSN. o Legal authorities may be found in the system's budget documents, information collection forms, or the program office's website. o You may be able to receive help from your OpDiv's Senior Official for Privacy, your OpDiv's Office of General Council, or the Departmental Privacy Act Officer in OS/ASPA. • The following authorities require that you complete a SORN or other documentation in order to use or disclose PII. Apart from rare exceptions, these authorities do not provide authority for a system to use or disclose PII and therefore should not be included in this response: o The Privacy Act of 1974; o The Freedom of Information Act; o The Federal Information Security Management Act; o The E-Government Act of 2002; o OMB Memorandum M-03-22; o The Health Information Portability and Accountability Act (HIPAA); or o The HIPAA Privacy and/or Security Rules located at 45 CFR Parts 160, 162, and 164. • Further information on legal authorities is covered in Appendix II: Legal Authorities.
Authorities and guidance:	• Public Law 93–579 Section 7 aka 5 USC § 552a (note) (page 1909): An agency requesting a SSN from an individual shall state what authority permits the solicitation of that SSN. • The Federal Register Document Drafting Handbook Section 3.5: A discussion on what authorities should be provided when publishing a notice in the Federal Register.
Skip logic:	• Q20a should only appear if the system contains PII (i.e., Q14 is marked yes).

Q21) Identify legal authorities governing information use and disclosure specific to the system and program.	
How to approach the question:	• If information collected or maintained in the system is subject to the Privacy Act, Q21 should include: o The legal authorities found in the cited SORNs that permit the use and disclosure of the information collected or maintained in the system; and o Any other legal authorities that govern the system's operations. • If information collected or maintained in the system is not subject to the Privacy Act: o Provide any legal authorities that reference the system and/or govern its operation; or o If no other authorities are known, you may cite to 5 USC 301, Departmental regulations.

Q21) Identify legal authorities governing information use and disclosure specific to the system and program.	
Additional considerations:	• How to find the legal authorities that govern the system: o Legal authorities may be found in the system's budget documents, information collection forms, SORNs or the program office's website. o You may be able to receive help from your OpDiv's Senior Official for Privacy, your OpDiv's Office of General Council, or the Departmental Privacy Act Officer in OS/ASPA. • The Privacy Act requires that each SORN cite at least one statute or Executive Order. For that reason, at least one statute or Executive Order listed in the authority section in each cited SORN should be relevant to the system and should be listed in answer to this question. o The scope of the system reviewed in a PIA may be different from the scope of the system of records addressed in a SORN. For this reason, not all authorities written in the SORNs cited in Q22a may be relevant to the system reviewed in the PIA (and therefore should not be listed in the PIA). Similarly, SORNs cited in Q22a may not include all the authorities which are relevant to a system reviewed in the PIA. o Although authorities such as the Code of Federal Regulations (CFR), Federal Register (FR), and HHS Memoranda may further explain the system and may be included, the key to answering this question is the relevant statue and/or Executive Order. • The following authorities require that you complete a SORN or other documentation in order to use or disclose PII. Apart from rare exceptions, these authorities do not provide authority for a system to use or disclose PII and therefore should not be included in this response: o The Privacy Act of 1974; o The Freedom of Information Act; o The Federal Information Security Management Act; o The E-Government Act of 2002; o OMB Memorandum M-03-22; o The Health Information Portability and Accountability Act (HIPAA); or o The HIPAA Privacy and/or Security Rules located at 45 CFR Parts 160, 162, and 164. • Further information on legal authorities is covered in Appendix II: Legal Authorities.

Q21) Identify legal authorities governing information use and disclosure specific to the system and program.	
Key terms:	• Systems of Records Notice (SORN): The Privacy Act requires that a SORN be published in the Federal Register to notify the public about a system of records. HHS SORNs are also available online. Although HHS may revise or create a new SORN, individuals generally have an opportunity to read and provide comments before that occurs. Each SORN will generally describe: o The types and sources of records in the system of records; o Who those records are about; o When, why, and where the records are used within the agency; o When, why, and where the records may be disclosed outside the agency without the individual's consent; o How the agency safeguards, stores, retrieves, accesses, retains, and disposes the records; o How an individual can make notification, access, and correction/amendment requests to the system of records' manager (called a System Manager); o The legal authorities for maintaining the system of records; and o If and how the system of records is exempt from certain Privacy Act requirements.
Authorities and guidance:	• Appendix I: SORNs and PIAs: Further explains the Privacy Act and lists several authorities related to the Privacy Act. • 5 USC 301, Departmental regulations: This authority states that the head of an Executive department may prescribe regulations for the government of his department, the conduct of its employees, the distribution and performance of its business, and the custody, use, and preservation of its records, papers, and property. In other words, each agency has some authority to create and maintain records in order to carry out the work of that agency.
Skip logic:	• Q21 should only appear if the system contains PII (i.e., Q14 is marked yes).

Q22) Are records in the system retrieved by one or more PII data elements?	
How to approach the question:	• Select yes if the system retrieves records about an individual by a direct personal identifier such that the Privacy Act applies.
Additional considerations:	• The goal of this question is to ask whether the Privacy Act applies. The Privacy Act does not include the term PII; it instead asks whether retrieval occurs by a name of an individual or… some identifying number, symbol, or other identifying particular assigned to an individual. Within HHS, this type of information is called a direct personal identifier. • Although this PIA/PTA Writers' Handbook generally explains what this question is seeking, your OpDiv's Senior Official for Privacy or the Departmental Privacy Act Officer in OS/ASPA can best assist you with any Privacy Act-related questions. • Further information on when the Privacy Act applies can be found in Appendix I: SORNs and PIAs under Privacy Act Basics – What Constitutes a System of Records. • This response should help fulfill the OMB M-03-22 Attachment A, Section C, requirement that a PIA analyze and describe whether a Privacy Act system of records is being created.
Key terms:	• Direct personal identifier: Information which is specific to a particular person. A birthday of someone who works for HHS is probably not a direct personal identifier. However, a birthday of someone who works for a particular office within a particular OpDiv may be a direct personal identifier.
Authorities and guidance:	• Appendix I: SORNs and PIAs: Further explains the Privacy Act and lists several authorities related to the Privacy Act.
Skip logic:	• Q22 should only appear if the system contains PII (i.e., Q14 is marked yes). • If Q22 is marked no, Q22a should disappear.

Q22a) 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.	
How to approach the question:	• If some or all of the PII collected or maintained in the system is subject to the Privacy Act: o List the assigned number and title of all applicable SORNs; o Select in progress if an applicable SORN is being developed; and o Select in progress if a listed SORN is being revised to match the system. • If none of the information collected or maintained in the system is subject to the Privacy Act, list not applicable in the first text box.
Additional considerations:	• Although the PIA/PTA Writers' Handbook generally explains what this question is seeking, your OpDiv's Privacy Act Officer, or the Departmental Privacy Act Officer within OS/ASPA, can best assist you in identifying existing or pending SORN(s) that cover, or could be revised to cover, the system. • Records stored in different systems may be subject to different SORNs. Be sure to only list the SORNs that apply to information maintained in the system being evaluated as part of the PIA. Avoid citing SORNs that only apply to information: o Before it is transferred into the system or; o After it has been disclosed from the system. • This response should help fulfill the OMB M-03-22 Attachment A, Section C, requirement that a PIA analyze and describe whether a system of records is being created according to the Privacy Act.
Authorities and guidance:	• Appendix I: SORNs and PIAs: Further explains the Privacy Act and lists several authorities related to the Privacy Act.
Skip logic:	• Q22a should only appear if: o The system contains PII (i.e., Q14 is marked yes); and o Records collected or maintained in the system, or shared with another system, are retrieved by one or more PII data elements (i.e., Q22 is marked yes).

Q23) Identify the sources of PII in the system.	
How to approach the question:	• Under the list that says: o Directly from an individual about whom the information pertains, select any methods by which individuals provide their own PII into the system. o Government sources, select any government sources that provide PII into the system. o Non-government sources, select any non-government sources that provide PII into the system. • A direct collection may result in the need to select one or more methods and one or more sources.
Additional considerations:	• Only select the proximate (most recent) source of PII. For example, if all PII collected or maintained in the system goes (1) from an individual (2) to a CMS system which is evaluated by a different PIA to (3) the CMS system covered by this PIA, check within the OpDiv, but not in-person. Collection of information directly from the individual to CMS should be evaluated in the first system's PIA. • The following are examples of what will usually be considered a direct collection of PII from an individual about whom the information pertains. The CMS employee in the examples is merely facilitating the direct collection. o An individual calls a CMS employee who manually enters the individual's responses into the system. o A CMS employee records responses from an individual into the CMS employee's personal notebook which are later entered into the system. o The individual faxes a document to CMS which is then scanned into the system. • Make sure to consider any PII collected into and/or maintained in the system in order to control system access. Please note that direct contractors using HHS credentials are considered HHS employees for the purposes of filling out the PIA form. For example: o In-Person and Within the OpDiv should be listed if PII is collected directly from CMS employees who are responsible for supporting a CMS system. o Online and Private Sector should be selected if private entities, such as health care providers, enter information into the system online. • This response should help fulfill the OMB M-03-22 Attachment A, Section C, requirement that a PIA analyze and describe what information is to be collected into and what opportunities individuals have to decline to provide information or to consent to particular uses of the information (other than required or authorized uses), and how that consent is granted.
Authorities and guidance:	• OMB M-03-22 Attachment A, Section C: States what should be evaluated in a PIA and when a PIA should commence. • Appendix I: SORNs and PIAs: Further explains the Privacy Act and lists several authorities related to the Privacy Act.
Skip logic:	• Q23 should only appear if the system contains PII (i.e., Q14 is marked yes).

Q23a) Identify the OMB information collection approval number and expiration date.	
How to approach the question:	• If information collected into the system is subject to one or more OMB Control Numbers: o List all the relevant numbers and their expiration dates; and o State of one or more approvals are pending. • If information collected into and/or maintained in the system is not subject to one or more OMB Control Numbers, the response should be not applicable.
Additional considerations:	• OMB Control Numbers are used for data collections subject to the Paperwork Reduction Act (PRA). The PRA applies to standardized information collections from more than 10 respondents. It does not apply to data collections from agencies, instrumentalities, or employees of the United States in their official capacities. • Generic clearances apply to some information collections. For more information: https://www.whitehouse.gov/sites/default/files/omb/assets/inforeg/PRA_Gen_ICRs_5-28-2010.pdf • In general, an approved OMB Control Number: o Is displayed on the paper or electronic form used to collect the information; and o Will expire after three years. • OMB hosts this website where users can search their database of current, expired, and pending OMB Control Numbers.
Authorities and guidance:	• 44 USC 3507 i.e. The Paperwork Reduction Act of 1995. • OMB Circular No. A-130 Revised Appendix IV: PRA requirements. • Frequently Asked Questions about PRA/ Information Collection.
Skip logic:	• Q23a should only appear if the system contains PII (i.e., Q14 is marked yes).

Q24) Is the PII shared with other organizations?	
How to approach the question:	• Select yes if any entities and individuals who are outside the OpDiv listed in Q1 have direct access to, or receive PII directly from, the system. • Select no if the: o System does not disclose PII; or o System only discloses PII to employees and systems of the OpDiv listed in Q1.
Additional considerations:	• Do not select yes if PII is only disclosed (1) from the system (2) to another system owned by that same OpDiv and then to (3) an external entity or individual. Disclosures outside the OpDiv should be evaluated in the PIA for that second system. • Please note that direct contractors using HHS credentials are considered HHS employees for the purposes of filling out the PIA form. •
Skip logic:	• Q24 should only appear if the system contains PII (i.e., Q14 is marked yes). • Q24a through Q24c should not appear unless PII collected or maintained in the system, or shared with another system, is disclosed to other organizations (i.e., Q24 is marked yes).

Q24a) Identify with whom the PII is shared or disclosed and for what purpose.	
How to approach the question:	• Select the types of entities and individuals who are outside the OpDiv listed in Q1 and have direct access to, or receive PII directly from, the system. • For each type selected: o Name or describe the entities or individual that have direct access to, or receive PII directly from, the system; and o Explain why each entity or individual has direct access to, or receives PII directly from, the system. For example, select Other Federal Agency/Agencies then write The Internal Revenue Service in order to determine whether an individual's reported income is below the maximum allowable amount to receive benefits.
Additional considerations:	Select Private Sector if some of the entities or individuals who receive or access the PII are contractors. Please note that direct contractors using HHS credentials are considered HHS employees for the purposes of filling out the PIA form. • The following terms mean that PII is disclosed to, or access is given to: o Within HHS: An HHS OpDiv not listed in Q1. o Other Federal Agency/Agencies: A part of the U.S. Federal Government that is not also part of HHS. o State or Local Agency/Agencies: A state and/or local government agency. o Private Sector: A contractor, business, non-profit organization, or other entity not covered above. • This response should help fulfill the OMB M-03-22 Attachment A, Section C, requirement that a PIA analyze and describe the intended use of the information and with whom the information will be shared.
Authorities and guidance:	• 5 USC 552a (i.e., The Privacy Act of 1974, as amended) Subsection (b): Indicates when records about an individual maintained in a system of records may be disclosed without first obtaining the individual's written consent. • Appendix I: SORNs and PIAs: Further explains the Privacy Act and lists several authorities related to the Privacy Act.
Skip logic:	• Q24a should only appear if: o The system contains PII (Q14 is marked yes); and o PII collected into and/or maintained in the system is disclosed to other organizations (Q24 is marked yes).

Q24b) 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)).	
How to approach the question:	• If PII in the system is shared or disclosed subject to one or more agreements, describe the sharing and disclosures that are permitted under each agreement. • If sharing or disclosure of PII in the system is not subject to an agreement, explain: o What sharing or disclosures are occurring without an agreement; and o Why no agreement is required or in place.
Additional considerations:	• The recipients described in this response should match the entities and individuals selected and described in Q24a. • This response should help fulfill the OMB M-03-22 Attachment A, Section C, requirement that a PIA analyze and describe: o The intended use of the information; o With whom the information will be shared; and o How the information will be secured.
Key terms:	• Computer Matching Agreement (CMA): The Privacy Act requires that a CMA be completed before records in a system of records may be electronically linked to records in another system of records, or non-federal records, in order to administer a federal benefit program, personnel system, or payroll system. The CMA documents and evaluates the privacy implications of that linkage. For example, there is a CMA because CMS and the Social Security Administration compare records in order to determine whether individuals qualify for certain income-based health insurance services. • Memorandum of Understanding (MOU): A document that establishes the terms and conditions for sharing information. It generally includes the reason for the sharing, the authorities that are relevant to the sharing, and the responsibilities of both organizations. The technical requirements will generally be documented in a related ISA. • Information Sharing Agreement (ISA): A document that establishes the technical requirements that are needed to share and protect electronic information. The purposes and legal requirements will generally be documented in a related MOU.
Authorities and guidance:	• 5 USC 552a (i.e., The Privacy Act of 1974, as amended): With regards to the CMA, subsection (a) includes relevant definitions, subsection (e) discusses publication requirements, and subsection (o) through (u) includes additional requirements. • OMB M-01-05, Guidance on Inter-Agency Sharing of Personal Data - Protecting Personal Privacy: Guidance on ISAs. • Appendix I: SORNs and PIAs: Further explains the Privacy Act and lists several authorities related to the Privacy Act.
Impact on the remaining PIA questions	• Q24b should only appear if: o The system contains PII (i.e., Q14 is marked yes); and o The PII collected or maintained in the system, or shared with another system, is disclosed to other organizations (i.e., Q24 is marked yes).

Q24c) Describe the procedures for accounting for disclosures.	
How to approach the question:	• If records in the system are subject to the Privacy Act, this answer should describe if and how HHS complies with Section (c), Accounting of Certain Disclosures. It requires HHS to maintain an accounting of disclosure with respect to all records in a system subject to the Privacy Act: o Every time HHS discloses a record outside HHS for a reason other than the Freedom of Information Act (FOIA), HHS is required to document: ▪ The date, nature, and purpose of each disclosure; and ▪ The name and address of the recipient. o HHS shall keep that document for five years after the disclosure occurred or the life of the record (whichever is longer). o If the individual named in the record requests an accounting of disclosures, HHS shall provide the details of all disclosures except for certain ones which relate to civil or criminal law enforcement. • If no records in the system are subject to the Privacy Act, this answer can be not applicable.
Additional considerations:	• This response should help fulfill the OMB M-03-22 Attachment A, Section C, requirement that a PIA analyze and describe with whom the information will be shared.
Authorities and guidance:	• 5 USC 552a (i.e., The Privacy Act of 1974, as amended) Subsection (c): A requirement to maintain an accounting of disclosures. • Appendix I: SORNs and PIAs: Further explains the Privacy Act and lists several authorities related to the Privacy Act.
Skip logic:	• Q24c should only appear if: o The system contains PII (i.e., Q14 is marked yes); and o The PII collected or maintained in the system, or shared with another system, is disclosed to other organizations (i.e., Q24 is marked yes).

Q25) Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason.	
How to approach the question:	• If the system collects information directly from an individual, the collection is governed by the Privacy Act, and the individual will receive a PAS (written, verbal, or otherwise) before or when their records are collected into the system: o Describe how and when the PAS is provided; and o Provide the text of the PAS (or a link to the PAS if will not fit in the textbox provided). • If the system collects information directly from an individual, the collection is governed by the Privacy Act, and the individual will not receive a PAS (written, verbal, or otherwise) before or when their records are collected into the system, describe why the PAS will not be provided. • If the system collects information directly from an individual, the collection is not governed by the Privacy Act, and the individual will still receive some type of notice (written, verbal, or otherwise): o State how and when the notice is provided; and o Provide the text of that notice or summarize what it includes. • If the system collects information directly from an individual, the collection is not governed by the Privacy Act, and the individual will not receive notice (written, verbal, or otherwise) before/when/after his/her PII is collected into the system, describe why the notice will not be provided. • Only consider whether an individual's PII will be collected from the individual directly into the system. If the system only collects PII from another system, the first system should provide the notice. An appropriate response would be "Not applicable. Notice is responsibility of the (please provide the name of the system or entity that collects information directly from an individual and supplies it to the system for which the PIA is about)."
Additional considerations:	• Since notice is a precursor to deciding whether to provide PII, this answer could discuss any opportunity to opt-out of the collection of PII. • If a notice is provided online, are there situations when the individual would not see it? o Could an individual visit the collection page without seeing the notice? o Would the notice appear if an individual utilizes a pop-up blocker? • A Privacy Act Statement may be provided in any format. • This response should help fulfill the OMB M-03-22 Attachment A, Section C, requirement that a PIA analyze and describe what opportunities individuals have to decline to provide information or to consent to particular uses of the information (other than required or authorized uses), and how that consent is granted.

Q25) Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason.	
Key terms:	• Privacy Act Statement (PAS): The notice that an agency is generally required to provide to an individual when his or her information is solicited for collection into a system of records. It includes a description of: o How the information may be used; o Where the information may be disclosed outside the agency; o The statute or Executive Order giving the agency the authority to request that information; o Whether the request for information is mandatory or voluntary (see Q26); and o What may happen to the individual if he or she does not provide part or all of the requested information.
Authorities and guidance:	• 5 USC 552a (i.e., The Privacy Act of 1974, as amended) Subsection (e)(3): The requirement to provide a PAS and what shall be included. • Appendix I: SORNs and PIAs: Further explains the Privacy Act and lists several authorities related to the Privacy Act.
Skip logic:	• Q25 should only appear if the system contains PII (i.e., Q14 is marked yes).

Q26) Is the submission of PII by individuals voluntary or mandatory?	
How to approach the question:	• Select mandatory if one's refusal to provide at least some of the PII maintained in the system may lead to a civil or criminal penalty. • Select voluntary in all other situations regardless of the repercussions that may result from one's refusal to provide the requested PII.
Additional considerations:	• OMB guidance on the Privacy Act explains that all requests are voluntary unless not providing the requested PII would lead to a civil or criminal penalty. There are situations in which the consequences for not providing one's PII could be job loss, withholding of health insurance, or other negative repercussions. Despite those repercussions, OMB still considers these decisions to be voluntary. • If an individual provides information in order to obtain a benefit or privilege, the government's request for information to process that benefit or privilege will be voluntary. • Although the PIA/PTA Templates do not provide an opportunity to comment, in Q26, you may detail elsewhere in the PIA (Q27 is one possible place): o What collections are voluntary verses mandatory; and/or o What repercussions will occur even though the request is voluntary. • This response should help fulfill the OMB M-03-22 Attachment A, Section C, requirement that a PIA analyze and describe what opportunities individuals have to decline to provide information or to consent to particular uses of the information (other than required or authorized uses), and how that consent is granted.
Authorities and guidance:	• OMB Privacy Act Implementation: Guidelines and Responsibilities, 40 FR 28962: An explanation of the differences between mandatory and voluntary.
Skip logic:	• Q26 should only appear if the system contains PII (i.e., Q14 is marked yes).

Q27) 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.	
How to approach the question:	• If there are situations in which the system requests PII from individuals and those individuals have the choice to opt-out of the use or collection of their PII, describe: o The opt-out processes; and o When those processes may be used. • If there are situations in which the system requests PII from individuals and those individuals do not have the choice to opt-out of the use or collection of their PII, describe: o When individuals cannot opt-out; and o The reason why individuals cannot opt-out. • In some situations, the answer may be that the individual was given the opportunity to opt-in to the collection hence no need to provide an opt-out. • Ifsystem that the PIA is about receives information from another system (a source system): If this system receives all information from another system (source system) and that system is therefore responsible for the providing methods for individuals to opt-out of the collection or use of their PII, please state as such, provide the name of the source system and indicate whether or not the PII in this source system is covered by a separate PIA.
Additional considerations:	• If PII maintained in the system is subject to the Privacy Act, then the Privacy Act prohibits that PII from being disclosed without the individual's prior written consent except for twelve reasons listed in the Privacy Act. The Privacy Act and the applicable SORN(s) cited in Q22a will contain guidance on what disclosures are permitted. • This response should help fulfill the OMB M-03-22 Attachment A, Section C, requirement that a PIA analyze and describe what opportunities individuals have to decline to provide information or to consent to particular uses of the information (other than required or authorized uses), and how that consent is granted.
Key terms:	• Opt-in: Individuals take affirmative action to allow the system to collect or use their PII. In other words, an individual's PII will not be collected and/or used unless that individual grants permission. • Opt-out: Individuals take affirmative action to prevent the collection or use of their PII. In other words, an individual's PII may be used or collected unless that individual specifically says otherwise. • Implied consent: Individuals implicitly consent to the use or collection of their PII through their behavior. For example, an individual enters a room with a sign on the wall that indicates that he or she may be video-recorded. If that individual remains in the room, he or she consents to being recorded.

Q27) 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.	
Authorities and guidance:	• OMB M-03-22: A requirement to review, as part of the PIA process, whether individuals may decline to provide information, or to consent to particular uses of their information (other than required or authorized uses), and how individuals can grant that consent. • 5 USC 552a (i.e., The Privacy Act of 1974, as amended) Subsections (b): Lists instances when records about an individual may be disclosed without the individual's prior written consent.
Skip logic:	• Q27 should only appear if the system contains PII (i.e., Q14 is marked yes).

Q28) 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.	
How to approach the question:	• Before an individual's PII will be used for a purpose materially different from that given at the time of collection, explain: o When and how notice will occur or why that will not occur; and o When and how individuals will have an opportunity to consent to the materially different purpose or why that will not occur. • If the system that the PIA is about receives information from another system (a source system): If this system receives all information from another system (source system) and that system is therefore responsible for the process to notify and obtain consent from the individuals whose PII is in the system when major changes occur to the system, please state as such, provide the name of the source system and indicate whether or not the PII in this source system is covered by a separate PIA.
Additional considerations:	• Since consent should only be acquired from an informed individual, this response should state whether the notice is clear and comprehensive. • This question evaluates what will occur if information is used for purposes that are different from those specified prior to or during collection. For example, what would happen before PII initially collected in order to process a new HHS employee is sold to an advertising firm? • If PII maintained in a system is subject to the Privacy Act, a SORN should describe some of the ways those records will be used within the agency and some of the reasons why the records may be disclosed to parties outside the agency. If a system will change in a way that will conflict with the SORN, a new or revised SORN may need to be published in the Federal Register. A 30-day public notice and comment period should elapse before the agency implements the changes reflected in the new SORN. • This response should help fulfill the OMB M-03-22 Attachment A, Section C, requirement that a PIA analyze and describe what opportunities individuals have to decline to provide information or to consent to particular uses of the information (other than required or authorized uses), and how that consent is granted.

Q28) 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.	
uthorities and guidance:	• 5 USC 552a (i.e., The Privacy Act of 1974, as amended) Subsections (e)(4) and (e)(11): Describes what shall be included in a SORN, when a new SORN shall be published, and a requirement to provide a comment period. • Appendix I: SORNs and PIAs: Further explains the Privacy Act and lists several authorities related to the Privacy Act.
Skip logic:	• Q28 should only appear if the system contains PII (i.e., Q14 is marked yes).

Q29) 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.	
How to approach the question:	• If a defined redress process gives individuals an opportunity to raise concerns that their PII in the system has been inappropriately obtained, used, or disclosed, the response to this question should: o State the name of the office that would handle those concerns; o Describe how an individual may raise questions or concerns; and o Describe how the concerns will be considered, investigated, and resolved. • If a defined process gives individuals an opportunity to raise concerns that their PII in the system is inaccurate, the response to this question should: o State the name of the office that would handle those concerns; o Describe how an individual may raise questions or concerns; and o Describe how the concerns will be considered, investigated, and resolved. • If there is not a defined process in place to address any of the situations, explain why such a process does not exist.
Additional considerations:	• If records in a system are subject to the Privacy Act, individuals will generally have the right to: o Find out if the system contains records about themselves, o Request access to their records; and o Request that their records be amended or corrected if they contain PII which is inaccurate, irrelevant, untimely, or incomplete.
Authorities and guidance:	• 5 USC 552a (i.e., The Privacy Act of 1974, as amended) Sections (d)-(f): A requirement to establish notification, access, and amendment procedures and to include them in the SORN. • Appendix I: SORNs and PIAs: Further explains the Privacy Act and lists several authorities related to the Privacy Act.
Skip logic:	• Q29 should only appear if the system contains PII (i.e., Q14 is marked yes).

Q30) 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.	
How to approach the question:	• Describe the processes in place, or explain why they do not exist, used to assure that PII in the system is periodically reviewed for: o Integrity; o Availability; o Accuracy; and o Relevancy.
Additional considerations:	• Describe any system processes which are designed to ensure that: o PII is not improperly or inadvertently modified or destroyed; o Individuals who provide or modify PII cannot repudiate that action; o PII is available when needed; o PII is sufficiently accurate for the purposes needed; and o Outdated, unnecessary, irrelevant, incoherent, and inaccurate PII is removed from the system. • This answer does not need to detail: o The National Archives and Records Administration (NARA) retention schedule for PII maintained in the system since that should be discussed in Q37; or o The system's security controls since that should be discussed in Q38. • If a system requires a SA, that SA may include a System Security Plan (SSP) containing the answer to this question. • If system records are subject to the Privacy Act, HHS is generally required to: o Maintain only those records which are relevant and necessary to accomplish the system's purpose as required by statue or Executive Order; o Ensure that all records used to make a determination about an individual are sufficiently accurate, relevant, timely, and complete to make a fair decision; o Ensure that all records disclosed outside the federal government for a reason other than FOIA are accurate, complete, timely, and relevant enough for HHS' purposes; and o Satisfy additional integrity, availability, accuracy, and relevancy requirements if the system is governed by a CMA.. • Your OpDiv's SOP, or other privacy personnel, may know about a regular review of the PII held by your OpDiv and any OpDiv-wide initiatives to eliminate unnecessary uses and collections of PII.
Key terms:	• Accuracy: Free of mistake or error. • Availability: Ensuring timely and reliable access to information. • Confidentiality: Preserving authorized restrictions on information access and disclosure. • Integrity: Information is not improperly modified or destroyed and one cannot dispute who provided or modified the information.

Authorities and guidance:	• 44 USC 3542, Definitions: The definitions of integrity and availability. • NIST FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems. • NIST FIPS Publication 200, Minimum Security Requirement for Federal Information and Information Systems. • OMB M-07-16 Attachment 1: A requirement to reduce the amount of collected PII to the minimum necessary. • HHS-OCIO-2011-0003, Revisions to the HHS-OCIO Policy for Information Systems Security and Privacy: Requires OpDiv SOPs to regularly review all PII held by their OpDiv and eliminate any unnecessary use or collection of PII. • 5 USC 552a (i.e., The Privacy Act of 1974, as amended) Section (e): Requires HHS to make sure that records in a system subject to the Privacy Act are relevant and necessary for an agency purpose required by law. It also says that, within reason, records which are: o Used to make a decision about an individual should be accurate, relevant, timely, and complete enough to make a fair decision; and o Disclosed to parties outside the agency should be accurate, complete, timely, and relevant for agency purposes. • 44 USC Chapter 33, Disposal of Records: Requirements regarding the disposal of federal records. • Appendix I: SORNs and PIAs: Further explains the Privacy Act and lists several authorities related to the Privacy Act.
Skip logic:	• Q30 should only appear if the system contains PII (i.e., Q14 is marked yes).

Q31) Identify who will have access to the PII in the system and the reason why they require access.	
How to approach the question:	• Select the types of individual who should have access to the PII maintained in the system. If a checkbox box is selected, describe the following in the associated textbox: o The PII that specific type of individual may access; and o The reason for granting that type of individual such access. • Select all relevant checkboxes, even if a type of individual matches more than one type. Please note that direct contractors using HHS credentials are considered HHS employees for the purposes of filling out the PIA form. • Do not select a checkbox if a type of individual should only have access to their own PII. For example, you should not select system users if the only PII they may access through the system is their own e-mail.
Additional considerations:	• A system user guide may indicate who should have access to what PII for what reason. • If a system requires a SA, that SA may include a System Security Plan (SSP) containing a description of user privileges.
Authorities and guidance:	• 44 USC 3542, Definitions: Confidentiality includes the need to restrict access. • OMB M-07-16: Limiting access to those who need such access reduces the risk of a breach. • NIST Special Publication 800-37 Revision 1, Information Security. • NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations. • NIST 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information: Considers the privacy impact of giving system users access to PII.
Skip logic:	• Q31 should only appear if the system contains PII (i.e., Q14 is marked yes).

Q32) Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII. **Q33) 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.**	
How to approach the question:	• For Q32, explain the administrative procedures used to determine why the categories of individuals described in Q31 should have access to PII maintained in the system. • For Q33, explain what system controls limit a user's access to the type, amount, or categories of PII necessary to perform their job functions as determined in Q32, or why those system controls do not exist.
Additional considerations:	• A system user guide may indicate who should have access to what PII for what reason and the process used to determine when a request for access should be granted. • If a system requires a SA, that SA may include a SSP containing a description of user privileges and a governance strategy to determine who should have access to what PII maintained in the system. • This response should help fulfill the OMB M-03-22 Attachment A, Section C, requirement that a PIA analyze and describe with whom the information will be shared and how the information will be secured.
Key terms:	• Principle of least privilege: Users' system access is limited to the functions and information which is essential to their job functions.
Authorities and guidance:	• 44 USC 3542, Definitions: Confidentiality includes the need to restrict access. • OMB M-07-16: Limiting access to those who need such access reduces the risk of a breach. • NIST Special Publication 800-37 Revision 1, Information Security. • NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations. • Controls for Federal Information Systems and Organizations. • NIST 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information: Considers the privacy impact of giving users access to PII.
Skip logic:	• Q32 through Q33 should only appear if the system contains PII (i.e., Q14 is marked yes).

Q34) 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.	
How to approach the question:	• If system users receive any general privacy and security training before and/or while they have access to the system, please describe: o The type, frequency, and topics of the trainings; and o The categories of users who receive each type of training.
Additional considerations:	• Examples of general user privacy and security awareness include: o Annual HHS Information Systems Security Awareness Training; o Annual HHS Privacy Training; and o Reading the Rules of Behavior for Use of HHS Information Resources and signing the accompanying acknowledgement. • Q34 asks what general privacy and security trainings are provided to system users while Q35 asks what training is provided to a type of system user because of their access to certain system information. If training seems to fit within both Q34 and Q35, you may select whether to discuss that training in either answer. • This response should help fulfill the OMB M-03-22 Attachment A, Section C, requirement that a PIA analyze and describe how the information will be secured.
Authorities and guidance:	• 44 USC 3544, Federal agency responsibilities: A requirement for federal agencies to provide security training to all personnel, including contractors, who have access to an information system used by that agency. • OMB M-07-16: Agencies should generally: o Provide privacy and security training to employees before they receive access to agency information and information systems; o Inform employees what to do when a security incident occurs; o Inform employees about the consequences of a violation; o Provide an annual privacy and security refresher course; and o Provide advanced training, if responsibilities increase or change.
Skip logic:	• Q34 should only appear if the system contains PII (i.e., Q14 is marked yes).

Q35) Describe training system users receive (above and beyond general security and privacy awareness training).	
How to approach the question:	• If system users receive any privacy and/or security awareness training because they have access to this particular system: o Describe the type, frequency, and content of those trainings; and o Specify which users receive which trainings. • If system users do not receive any privacy and security trainings specifically because they have access to this particular system, write not applicable.
Additional considerations:	• If records maintained in the system are subject to the Privacy Act, HHS is generally required to: o Establish rules of conduct for individuals who design, develop, operate, or maintain those records; and o Inform those individuals about the rules of conduct and the punishments that should occur if those rules are violated. • Training can be delivered in many forms. o They may occur in person, online, via a teleconference, et cetera. o They may take the form of a manual, handbook, PowerPoint slide presentation, event, poster, e-mail blast, et cetera. • Q34 asks what general privacy and security trainings are provided to system users while Q35 asks what training is provided to a type of system user because of their access to certain system information. If training seems to fit within both Q34 and Q35, you may select whether to discuss that training in either answer. • This response should help fulfill the OMB M-03-22 Attachment A, Section C, requirement that a PIA analyze and describe how the information will be secured.
Authorities and guidance:	• 5 USC 552a (i.e., The Privacy Act of 1974, as amended) Subsections (e)(9) and (i)(1): A requirement to establish and disseminate rules of conduct for individuals with access to records in a system subject to the Privacy Act as well as penalties for noncompliance • 44 USC 3544(a), Federal agency responsibilities Section (a): A requirement that federal agencies are responsible for providing security training to all personnel, including contractors, who have access to an information system used by that agency. • OMB M-07-16 Attachment 1: A requirement to provide additional or advanced privacy and security training when there is an increase in responsibilities or a change in duties. • Appendix I: SORNs and PIAs: Further explains the Privacy Act and lists several authorities related to the Privacy Act.
Skip logic:	• Q35 should only appear if the system contains PII (i.e., Q14 is marked yes).

Q36) Do contracts include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices?	
How to approach the question:	• This answer should be yes if one or more appropriate clauses are needed and included: o Contractors and/or subcontractors will have access to PII via an electronic system such that the contract should and does include HHS Acquisition Regulation (HHSAR) Clauses 352.239-72; and/or o Contractors and/or subcontractors will have access to records in a system subject to the Privacy Act such that the contract should and does include HHSAR Clauses 352.224-70. • This answer should be no if: o No FAR clauses are needed; or o FAR clause are needed yet not included. Other questions such as Q31 will allow readers and reviewers to determine whether no in this PIA indicates a compliance concern or that the clauses are unnecessary.
Additional considerations:	• The Privacy Act dictates how federal agency officials and employees may handle records maintained in a system which are subject to the Privacy Act, but does not apply to agency contractors and subcontractors who handle those same records. Subsection (m) of the Privacy Act says any contract which gives contractors access to those records should include provisions which make the contractor legally liable for not following many of the rules that federal agency officials and employees are required to follow. • This response should help fulfill the OMB M-03-22 Attachment A, Section C, requirement that a PIA analyze and describe how the information will be secured.
Key terms:	• Federal Acquisition Regulation (FAR): Primary regulation used by all federal agencies when contracting for supplies and services with appropriated funds. • HHS Acquisition Regulation (HHSAR): The standard contract clauses in HHS contracts which implement and supplement the FAR.
Authorities and guidance:	• 5 USC 552a (i.e., The Privacy Act of 1974, as amended) Section (m): Requires a federal agency to ensure through contract that certain Privacy Act provisions apply to contractors as if they were federal employees when given access to records in a system subject to the Privacy Act. • The HHSAR includes Part 324, Protection of Privacy and Freedom of Information: o HHSAR 324.103(b)(2): A requirement to incorporate HHSAR clauses when a contract involves records in a system subject to the Privacy Act and makes contractors/subcontractors aware of the applicable privacy requirements. o HHSAR 352.224-70: Required to be included in HHS contracts that give contractors access to records in a system subject to the Privacy Act. o HHSAR 352.239-72: Required to be included in HHS contracts that give contractors access to PII via an electronic systems which are not for national security purposes.
Skip logic:	• Q36 should only appear if the system contains PII (i.e., Q14 is marked yes).

Q37) Describe the process and guidelines in place with regard to the retention and destruction of PII. Cite specific records retention schedules.	
How to approach the question:	• This response should: o List any of NARA's Records Control Schedule (RCS) Job Numbers or General Records Schedules (GRSs) that apply to the PII maintained in the system; and/or o State if NARA is determining the appropriate RCS Job Number or GRS for some or all of the PII maintained in the system and that the PII should be maintained until a determination is provided.
Additional considerations:	• Although the PIA/PTA Writers' Handbook explains what this question is seeking, your OpDiv's Records Officer can best assist you with any records retention-related questions. • RCS Job Numbers generally include short combinations of letters and numbers connected with dashes. • NARA's webpage with information on all RCS Job Numbers and GRSs. • When viewing a Standard Form (SF) 115, Request for Records Disposition Authority: o The RCS Job Number is located in the top right text box; and o The remainder of the form should include a description of the records and their proposed disposition. • Other information about records retention, such as the text of the records retention section written in a SORN, does not replace the need to provide RCS Job Numbers, GRSs, an explanation of when one or more will be assigned, and/or an explanation of why one or more will not be assigned.
Key terms:	• National Archives and Records Administration (NARA): Responsible for assisting agencies with the creation of, and responsible for approving, retention disposition schedules that authorize the destruction of federal records. • Records Control Schedule (RCS): A NARA-approved document which states the duration of time a record should be maintained before it should be destroyed (subject to litigation, audits, and other holds). • General Records Schedule (GRS): A NARA-approved records retention schedule that applies to a certain type of records that is common to more than one agency.

Q37) Describe the process and guidelines in place with regard to the retention and destruction of PII. Cite specific records retention schedules.	
Authorities and guidance:	• OMB Circular No. A-130 Revised: requires agencies to: o Obtain a NARA approved retention schedules for all federal records; and o Provide training and guidance as appropriate to all agency officials, employees, and contractors regarding their federal records management responsibilities. • 36 CFR 1228, Disposition of Federal Records: The policies, standard procedures, and techniques for disposing of all federal records created or acquired by a federal agency. • The Standard Form (SF) 115 and instructions. • Records Schedules Frequently Asked Questions. • Parts of the CFR which affect NARA. • About Records Control Schedules and the Repository. • NARA's Records Management Publications.
Skip logic:	• Q37 should only appear if the system contains PII (i.e., Q14 is marked yes).

Q38) Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.	
How to approach the question:	• This response should provide a high-level overview of the system's administrative, technical, and physical security controls, a few examples of each control may be appropriate (use of passwords, a clearance is required).
Additional considerations:	• Response may be subdivided by: o Administrative, technical, and physical control; or o The families established in NIST Special Publication 800-53 Revision 4. • If records are in a system subject to the Privacy Act, HHS is generally required to establish appropriate administrative, technical, and physical safeguards to protect the records from anticipated threats or hazards. • Since this response will be published, it should not provide such specific information that it compromises system security. For example, stating that the server is protected in a building patrolled by armed guards is appropriate, but we recommend not specifying how many guards may be present, where they are located, etc. • This response should help fulfill the OMB M-03-22 Attachment A, Section C, requirement that a PIA analyze and describe how the information will be secured.
Key terms:	• Administrative controls: Administrative actions, policies, and procedures designed to manage (1) the selection, development, implementation, and maintenance of the security measures designed to protect the PII and (2) the conduct of those with access to the PII. o Includes: Training requirements, sanction policy, risk analysis, and log-in monitoring. • Technical controls: The technology, policies, and procedures used to protect the PII and control access to the PII. o Includes: Encryption, automatic logoff, and 2-factor authorization. • Physical controls: The physical measures, policies, and procedures designed to protect electronic information systems, buildings, and equipment from unauthorized intrusions, environmental hazards, and natural hazards. o Includes: Facility access controls and disposal controls.
Authorities and guidance:	• 5 USC 552a (i.e., The Privacy Act of 1974, as amended) Subsection (e)(10): A requirement to establish administrative, technical, and physical safeguards. • HIPAA Security Rule: Source of the administrative, technical, and physical control definitions listed above (called safeguards within HIPAA instead of controls). • OMB M-07-16 Attachment 1: A requirement to create a security program to protect PII and the five security requirements that agencies should implement: encryption, control remote access, time-out function, log and verify, and ensure understanding of responsibilities. • NIST Special Publication 800-53 Revision 4. • Appendix I: SORNs and PIAs: Further explains the Privacy Act and lists several authorities related to the Privacy Act.
Skip logic:	• Q38 should only appear if the system contains PII (i.e., Q14 is marked yes).

Q39) Identify the publicly-available URL:	
How to approach the question:	• Provide a link to the main page of any website which is: o Available to and for the use of the general public; and o Part of the system being reviewed by this PIA. • If a URL is unavailable because a website is not yet available to the general public, state that the website is currently in the development stage, but do not provide the URL of the development website.
Additional considerations:	• Do not provide links to websites which are only used for: o Internal agency activities (such as on intranets, internal applications, or interactions that only involve HHS employees and/or contractors directly supporting HHS); or o Activities that involve authorized law enforcement, national security, or national intelligence. • Do not provide links to websites if only employees and/or contractors directly supporting HHS who receive login credentials will be able to view anything beyond the login page.
Key terms:	• Uniform Resource Locator (URL): A website address such as http://www.hhs.gov/.
Authorities and guidance:	• E-Government Act Section 208. • OMB M-03-22 Attachment A, Section III, Privacy Policies on Agency Websites: Guidance on the need to have a privacy policy when a federal agency operates a website which is available to the public. • OMB M-10-22 Attachment 1: Guidance on the use of web measurement and customization technologies when a federal agency operates a website. • OMB M-99-18: A requirement to post clear privacy policies on websites (partially superseded by later OMB requirements).
Skip logic:	• Q39 should only appear if the system includes a website available to and for the use of the general public (i.e., Q4 is marked yes).

Q40) Does the website have a posted privacy notice?	
How to approach the question:	• For the purposes of this question, website refers to a system's website available to and for the use of the general public as described in Q39. • Select yes if a privacy notice that complies with all E-Government Act and OMB Memoranda is posted on: o All known major entry points (regardless of whether PII is collected); and o All pages that collects substantial personal information from the public.
Additional considerations:	• When responding to this question, do not consider whether the website collects information into a system subject to the Privacy Act and provides a PAS. This question is only asking about the website-specific privacy notifications that are required by the E-Government Act and OMB Memoranda. • Privacy notice requirements are based on the authorities listed below. Among other requirements, the notice should: o Be clearly labeled and easily accessed by a visitor; o Be clear and concise; o Be written in plain language; o Describe what information is collected from an individual, why it is collected, how it is used, where it is disclosed, whether one can opt-in or out-out of the collection, and how it is secured; o Describe whether the request for information is voluntary and how the website may obtain consent for non-mandatory collections; o Describe any use of website measurement and customization technologies or IP address logging; and o Describe how PII is handled when submitted via e-mail or a web form hosted by the system's website.
Authorities and guidance:	• E-Government Act Section 208(c): Requirements for federal agency website privacy policies. • OMB M-99-18, A requirement to post clear privacy policies on websites (partially superseded by later OMB requirements). • OMB M-03-22 Attachment A, Section III, Privacy Policies on Agency Websites: Guidance on the need to have a privacy policy when a federal agency operates a website which is available to the public. • OMB M-10-22 Attachment 1: Guidance on the use of web measurement and customization technologies when a federal agency operates a website. • OMB M-10-23: Guidance on privacy policies when a federal agency utilizes third party websites and applications.
Skip logic:	• Q40 should only appear if the system includes a website available to and for the use of the general public (i.e., Q4 is marked yes). • If Q40 is marked no, Q40a should not appear on the form.

Q40a) Is the privacy policy available in a machine-readable format?	
How to approach the question:	• Select yes if all the system's websites that are available to and for the use of the general public include a machine-readable privacy policy that complies with all E-Government Act and OMB Memoranda.
Additional considerations:	• A machine-readable privacy policy should: o Be included on any website that requires a human-readable privacy policy; and o Include the information required in a human-readable policy (See Q40).
Key terms:	• Machine-readable privacy policy: A document which lists a website's privacy practices in a language that can be read and understood by an internet browser. When placed on a website, the internet browser can automatically compare the website's privacy practices to the visitor's preset preferences and inform the visitor whether or not there are differences between the two. • Platform for Privacy Preferences (P3P): The standard vocabulary that should be used to write all machine-readable privacy policies placed on a federal agency's website.
Authorities and guidance:	• Public Law 107–347 i.e., E-Government Act of 2002 Section 208(c)(2): A requirement that federal agencies translate privacy policies into standardized machine-readable format. • OMB M-03-22 Attachment A, Section IV, Privacy Policies in Machine-Readable Formats. • HHS-OCIO-2010-0001 Policy for Machine-Readable Privacy Policies. • HHS OCIO 2009-0002.001, Policy for Privacy Impact Assessment (PIA) Section 5.2.6: A requirement that owners/administrators be responsible for implementing machine-readable privacy policies. • HHS Machine-Readable Privacy Policy Guide and the Privacy Policy Machine Readable Training (PDF on intranet). • Data.gov: A Primer on Machine Readability for Online Documents and Data.
Skip logic:	• Q40a should only appear if: o The system includes a website available to and for the use of the general public (i.e., Q4 is marked yes); and o The website has a posted privacy notice (i.e., Q40 is marked yes).

Q41) Does the Website use web measurement and customization technology?	
How to approach the question:	• Indicate whether any of the system's websites, which are available to and for the use of the general public, use any web measurement and customization technologies. • Web measurement and customization technology includes: o Temporary and permanent cookies; o Web bugs / beacons; and o Any other technology used to remember a user's online interactions with a website in order to conduct measurement and analysis of usage or to customize the user's experience.
Additional considerations:	• HHS and its contractors are not allowed to use persistent tracking technology on any HHS website for the general public unless: o The technology meets all conditions listed in OMB M-10-22; and o The HHS SAOP approves a written request to use that technology. • In Internet Explorer 9, you can view all cookies linked to a website by; o Opening the website in your browser; o Clicking on safety or view; and then o Clicking webpage privacy policy… If the cookies column in the table says either accepted or blocked, the website uses cookies. Which cookies are accepted or blocked may vary based on the browser's privacy settings.
Key terms:	• Web measurement and customization technology: Technology used to remember a user's online interactions with a website in order to measure and analyze usage or customize a user's experience.
Authorities and guidance:	• OMB M-10-22: Several requirements regarding a federal agency's use of web measurement and customization technologies. • HHS Memorandum, Implementation of OMB M-10-22 and M-10-23.
Skip logic:	• Q41 should only appear if the system includes a website available to and for the use of the general public (i.e., Q4 is marked yes). • If Q41 is marked no, Q41a should no longer appear on the form.

Q41a) Select the type of website measurement and customization technologies is in use and if it is used to collect PII. (Select all that apply)	
How to approach the question:	• Select the types of web measurement and customization technologies used by the system's websites that are available to and for the use of the general public. • For each type of technology selected, select whether it collects PII.
Additional considerations:	• A web beacon and a web bug are the same thing; you may select one and leave the other blank. • This response should help fulfill the OMB M-03-22 Attachment A, Section C, requirement that a PIA analyze and describe what information is to be collected.
Key terms:	• Web beacon (i.e., web bug): A small graphic in a webpage or e-mail that allows a server to track a user's online activity or verify if the user has viewed a particular webpage or e-mail. o Example: You receive an e-mail from Store-X that contains several pictures. Each time you open the e-mail, Store-X's server sends the pictures to your e-mail. Store-X can count how many times the pictures are sent, which indicates the number of times the e-mail was read. • Persistent cookie: A small file placed on a user's computer for a variable length of time when a website is visited. It can be used to gather information about the user and remember the user when he or she returns to the website via the same computer. o Example: You visit Store-X's website and search for baby goods. Store-X places a persistent cookie on your computer that will expire in 90 days and is tagged as baby goods. If you use the same computer to revisit Store-X's website within 90 days, Store-X will infer from the persistent cookie that you may be more interested in baby goods and should advertise them on the main page. o Example: You visit Website-X and indicate that you want to read the website in English. If Website-X places a persistent cookie on your computer which indicates English, Website-X will default to English every time you open the website on that computer. • Session cookie: A small file placed on a user's computer when a website is visited that will only remain until the browser is closed. o Example: You visit Website-Y and increase the size of the website's text. If Website-Y places a session cookie on your computer, the text of Website-Y will remain larger until you close the browser. When you return to Website-Y, the text will be smaller again.
Authorities and guidance:	• OMB M-10-22: Several requirements regarding a federal agency's use of web measurement and customization technologies. • HHS Memorandum, Implementation of OMB M-10-22 and M-10-23.
Skip logic:	• Q41a should only appear if: o The system includes a website available to and for the use of the general public (i.e., Q4 is marked yes); and o The website uses web measurement and customization technology (i.e., Q41 is marked yes).

Q42) Does the website have any information or pages directed at children under the age of thirteen?	
How to approach the question:	• Select whether the system's website, available to and for the use of the general public, contains any information or pages directed at children under the age of thirteen, such that it would be subject to the Children's Online Privacy Protection Act of 1998 (COPPA).
Additional considerations:	• COPPA imposes certain requirements on owners and operators of websites which are directed at children less than 13 years of age. • The Federal Trade Commission (FTC): o Published a webpage which explains COPPA and includes several related authorities. o Published a supplemental FAQ which explains how to determine whether a website is subject to COPPA. o Will answer questions or comments relating to COPPA which are sent to (CoppaHotLine@ftc.gov).
Authorities and guidance:	• 5 USC 6501–6505, Children's Online Privacy Protection Act of 1998. • 15 USC Chapter 91, Children's Online Privacy Protection. • 16 CFR Part 312, Children's Online Privacy Protection Rule: Final Rule Amendments to Clarify the Scope of the Rule and Strengthen its Protections for Children's Personal Information. • OMB M-03-22 Attachment C: A summary of COPPA requirements and extends COPPA applicability to federal agency websites.
Skip logic:	• Q42 should only appear if the system includes a website available to and for the use of the general public (i.e., Q4 is marked yes). • If Q42 is marked no, Q42a should no longer appear on the form.

Q42a) 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?	
How to approach the question:	• Select whether the websites, referenced in Q42, include a privacy policy that satisfies all COPPA requirements.
Additional considerations:	• COPPA states that specific content should be included in a website's privacy policy when that website is subject to COPPA.
Authorities and guidance:	• 5 USC 6501–6505, Children's Online Privacy Protection Act of 1998. • 15 USC Chapter 91, Children's Online Privacy Protection. • 16 CFR Part 312, Children's Online Privacy Protection Rule: Final Rule Amendments to Clarify the Scope of the Rule and Strengthen its Protections for Children's Personal Information. • OMB M-03-22 Attachment C: A summary of COPPA requirements and extends COPPA applicability to federal agencies' websites.
Skip logic:	• Q42 should only appear if: o The system includes a website available to and for the use of the general public (i.e., Q4 is marked yes); and o Any of those websites has any information or pages directed at children under the age of thirteen (i.e., Q42 is marked yes).

Q43) Does the website contain links to non-federal government websites external to HHS?	
How to approach the question:	• If the system includes a website available to and for the use of the general public which is controlled by the federal government, select whether it links to any websites available to and for the use of the general public which are not controlled by the federal government.
Key terms:	• Link: Any text, pictures, selectable boxes, and other features that redirect individuals away from the page they are currently viewing.
Authorities and guidance:	• OMB M-10-23(3)(b): A requirement to post a notice when a link on an agency website will lead to a website which is not owned by the federal government. That notice should indicate that the user is being directed to a nongovernment website which may not have the same privacy policies as the federal agency website. • HHS Memorandum, Implementation of OMB M-10-22 and M-10-23 Section 7: The requirement to provide the notice and provides sample alert language.
Skip logic:	• Q43 should only appear if the system includes a website available to and for the use of the general public (i.e., Q4 is marked yes). • If Q43 is marked no, Q43a should no longer appear on the form.

Q43a) Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?	
How to approach the question:	• Select whether or not an individual will see an alert which says they are moving from a website which is controlled by the federal government to a website when is not controlled by the federal government every time they click one of those links which led to yes being selected in Q43.
Additional considerations:	• The alert could be a statement, appearing adjacent to the link or a pop-up, which says that viewers are being directed to a website which is not controlled by the federal government and may have different privacy policies from those of the agency's official website. • Sample alert language: *This hyperlink will direct you to a non-governmental website or application. The appearance of external hyperlinks does not constitute an endorsement by the United States Department of Health & Human Services (HHS) of the hyperlinked website or application, or the information, products, or services contained therein. Visitors to the hyperlinked website or application will be subject to that website or application's privacy policies. These practices may be different than those of this HHS website.*
Authorities and guidance:	• OMB M-10-23(3)(b): A requirement to post a notice when a link on an agency website will lead to a website which is not owned by the federal government. That notice should indicate that the user is being directed to nongovernment website which may not have the same privacy policies as the federal agency website. • HHS Memorandum, Implementation of OMB M-10-22 and M-10-23 Section 7: A requirement to provide the notice and provides sample alert language.
Skip logic:	• Q43a should only appear if: o The system includes a website available to and for the use of the general public (i.e., Q4 is marked yes); and o The website contains one or more links to a website which is not owned by HHS (i.e., Q43 is marked yes).

Appendix I: SORNs and PIAs

Introduction:
The E-Government Act states that a PIA should evaluate whether a system being reviewed for PIA purposes is also subject to the Privacy Act. For this reason, the PIA/PTA Writers' Handbook includes this general summary of the Privacy Act as it relates to the PIA. For further information on Privacy Act applicability and requirements, please consult your OpDiv's Senior Official for Privacy and/or the Departmental Privacy Act Officer in OS/ASPA.

Privacy Act Basics – What Constitutes a System of Records:
The Privacy Act protects information about an individual when stored in a system of records. A system of records is created when:

- A group of records (electronic or paper);
- Maintained by an agency or a contractor on behalf of an agency;
- Contain information about an individual;
- Which is retrieved by a direct personal identifier.

A few comments on the above statement:

- The retrieval has to actually happen; merely having the capacity to retrieve will not trigger the Privacy Act.
- The direct personal identifier is something that can directly identify an individual. A name or driver's license number is usually considered a direct personal identifier, while a case or file number would probably not be considered as such.
- The retrieval by a direct personal identifier has to occur in the first instance (i.e., by name then date) verses a later instance (i.e., by date then name).
- Deliberately structuring a system to avoid the Privacy Act is not permitted.

An example of what would probably:

- Create a system of records: HHS collects the names of individuals and their addresses into a database, and then searches the database by a name to retrieve an address.
- Not create a system of records: HHS collects the names of individuals and the dates of their medical appointments into a database, and then searches the database by a date to determine who had a medical appointment on a particular day.

In the first example, a system of records is probably created because HHS uses a direct personal identifier (an individual's name) to retrieve more information about that individual. In the second example, a system of records is probably not created because HHS retrieved by information that is not a direct personal identifier (a date of an appointment). The second example could become a system of records if someone's name was used to retrieve the date of their appointment, but not until that actually occurs.

Privacy Act Documents:
The Privacy Act protects the privacy of those with information maintained in a system of records by requiring certain documents to be created and provided to the public. This includes:

- An accurate SORN prior to operating a system of records;
- A PAS when soliciting information from individuals for collection into a system of records;
- A CMA before using records from a system of records in a matching program; and
- An accounting of disclosures, compiled as disclosures are made from the system of records.

Key Differences between SORNs and PIAs:
Since the need to publish SORNs and PIAs is discussed in the same context, it is helpful to note some major differences between SORNs and PIAs:

	System of Records Notice	Privacy Impact Assessment
Key legal requirements:	Privacy Act of 1974 (as amended), OMB Circular No. A-130	E-Government Act of 2002, OMB M-03-22
Key terminology:	Records about individuals, System of records, Direct personal identifier	Personally identifiable information, Electronic information systems and collections
Applies to information in:	Electronic and/or paper form	Only electronic form
Coverage:	A SORN can cover records in multiple electronic systems.	A separate PIA is generally required for each system.

In other words, a PIA may describe an entire system of records, part of a system of records, or more than what is in a system of records. Similarly, a SORN may describe the system evaluated in a PIA, part of a system, or more than just one system. For this reason, not everything written in a SORN may match a PIA and not everything written in a PIA may match a SORN.

Privacy Act Authorities:

- 5 USC 552a (i.e., The Privacy Act of 1974, as amended).
- OMB M-03-22 Attachment A, Section C: States that a PIA should analyze and describe whether a system of records is being created according to the Privacy Act.
- OMB Circular No. A-130 Revised Appendix I: Agency responsibilities regarding the Privacy Act.
- 45 CFR 5b, Privacy Act Regulations: Privacy Act requirements within HHS.
- Public HHS website that discusses the Privacy Act.
- HHS OCIO 2009-0002.001, Policy for Privacy Impact Assessment (PIA), Section 5.1.2: Discusses the HHS Privacy Act Officer within the Office of the Assistant Secretary for Public Affairs (ASPA).
- The Overview of the Privacy Act of 1974 as prepared by the Department of Justice's Office of Privacy and Civil Liberties.

Appendix II: Legal Authorities

Executive Orders (EO)	
Background:	• Executive Orders (EOs) are official documents, numbered consecutively, that have been signed by the President and published in the Federal Register.
General Guidance:	• EOs have the full force of law and may be used as a legal authority.
Citation conventions:	• EO 9397, Numbering System for Federal Accounts Relating to Individual Persons. • Executive Order 13478, Amendments To Executive Order 9397 Relating To Federal Agency Use of Social Security Numbers.

United States Code (USC)	
Background:	• The United States Code (USC) is a collection of the federal laws of the United States that are organized by subject matter and updated regularly.
General Guidance:	• This is the citation that is generally expected when a question requests a statute or statutory authority. • USC citations generally reference an entire chapter or relevant sections. • Titles and Volumes are the equivalent of a chapter in a book. Therefore, citing Title X or Volume Y without providing further information is the equivalent of providing a chapter name without including the name of the book.
Citation conventions:	• Examples of a chapter citation: o 5 USC Chapter 3, Powers. o 5 USC Chap. 3, Powers. • Examples of a section citation: o 5 USC Section 301, Departmental regulations. o 5 USC § 301, Departmental regulations.

Public Laws (PL)	
Background:	• Public Laws (PLs) refer to the original text of laws which have been approved by both houses of Congress and the President.
General Guidance:	• PLs should not be cited when possible: o Many PLs are a long list of changes which dictate how sections of the USC should be modified. Compared to the updated USC citation, which shows the statute with the changes established, it is very difficult to understand what a Public Law is designed to accomplish. o Unlike the USC, which is published on several different internet websites, older PLs can be very difficult to find.
Citation conventions:	• PL 900-359, Name of Fictitious PL • Pub-Law, Name of Fictitious Citation Pub-Law.

Code of Federal Regulations (CFR)	
Background:	• The CFR is a consolidated record of the rules published by federal departments and agencies in the Federal Register.
General Guidance:	• CFRs are not considered statutes so they will generally not provide authority to collect the SSN or collect records into a system of records. However, sections of the CFR are often created under the direction of a statute, and further detail what a statute is designed to accomplish, so they may be helpful to the reader. • CFR citations generally reference an entire chapter or the relevant sections.
Citation conventions:	• Examples of a chapter citation: o 80 CFR Chapter 99, Name of Fictitious Chapter. o 80 CFR Chap. 99, Name of Fictitious Chapter. Examples of a section citation: o 80 CFR Section 999, Name of Fictitious Section o 80 CFR § 999, Name of Fictitious Section

The Federal Register (FR)	
Background:	• The Federal Register is used by the federal government announce new documents including proposed rules, final rules, public notices, and Presidential actions.
General Guidance:	• Most publications in the Federal Register are not considered a statute or EO and will generally not provide authority to collect the SSNs or records into a system of records. However, sections of the Federal Register are often created under the direction of a statute, and further detail what a statute is designed to accomplish, so they may be helpful to the reader. • Final rules distributed by a federal agency and published in Federal Register are later re-published in the CFR, which is updated annually. • Some of these authorities are similar to PLs in that they are the change orders that result in a new or modified section of the CFR.
Citation conventions:	• 99 FR 99999, Name of Fictitious Publication.

Appendix III: Useful Acronyms

Acronym	Name
ATO	Authority to Operate
C&A	Certification & Accreditation
CFR	Code of Federal Regulations
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CMA	Computer Matching Agreement
COPPA	Children's Online Privacy Protection Act
EPLC	Enterprise Performance Life Cycle
FAR	Federal Acquisition Regulation
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
FR	Federal Register
FTC	Federal Trade Commission
GRS	General Records Schedules
GSS	General Support System
HEAR	HHS Enterprise Architecture Repository
HIPAA	Health Information Portability and Accountability Act
HSDW	HHS Security Data Warehouse
HHS	Department of Health and Human Service
HHSAR	HHS Acquisition Regulation
ICR	Information Collection Request
ISA	Information Sharing Agreement
ISSO	Information System Security Officer
IT	Information Technology
MOU	Memorandum of Understanding
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OIG	Office of the Inspector General
OMB	Office of Management and Budget
OpDiv	Operating Division
OS	Office of the Secretary
OS/ASPA	Office of the Assistant Secretary for Public Affairs
PAS	Privacy Act Statement
PIA	Privacy Impact Assessment
PTA	Privacy Threshold Analysis

PII	Personally Identifiable Information
PL	Public Laws
POC	Point of Contact
PRA	Paperwork Reduction Act
P3P	Platform for Privacy Preferences
Q	Question
RCS	Records Control Schedule
SAOP	Senior Agency Official for Privacy
SA	Security Authorization
SA&A	Security Assessment & Authorization
SF	Standard Form
SOP	Senior Official for Privacy
SORN	System of Records Notice
SSN	Social Security Number
SSP	System Security Plan
StaffDiv	Staff Division
URL	Uniform Resource Locator
USC	United States Code
UUID	System Universal Unique Identifier

Appendix IV: Useful Terminology

Access control software: Software that authenticates a user's credentials before they are given access to an intended system or resource such as this example of CMS's Identity & Access Management System.

Accuracy: Free of mistake or error.

Administrative controls: Administrative actions, policies, and procedures designed to manage (1) the selection, development, implementation, and maintenance of the security measures designed to protect the PII and (2) the conduct of those with access to the PII.

Alteration in Character of Data: New PII will be added to a system and that will cause a new privacy risk. For example, health or financial information will be added to a system that currently contains only contact information. (OMB M-03-22 Attachment A provides examples of what system changes could result in a new privacy risk and therefore require an update to an existing PIA. Although this term is the same as that in M-03-22, the definition has been revised for clarity).

Anonymous to Non-Anonymous: Anonymous information stored in a system will be changed into PII. For example, a system containing survey results, which are currently linked to an anonymous identifier, will be linked to PII. (OMB M-03-22 Attachment A provides examples of what system changes could result in a new privacy risk and therefore require an update to an existing PIA. Although this term is the same as that in M-03-22, the definition has been revised for clarity).

Availability: Ensuring timely and reliable access to information.

Commercial Sources: PII purchased or obtained from commercial or public sources will be added to a system on a regular basis. Note that adding commercial or publicly acquired PII to a system on an ad hoc basis is not considered a new privacy risk. (OMB M-03-22 Attachment A provides examples of what system changes could result in a new privacy risk and therefore require an update to an existing PIA. Although this term is the same as that in M-03-22, the definition has been revised for clarity).

Computer Matching Agreement (CMA): The Privacy Act requires that a CMA be completed before records in a system of records may be electronically linked to records in another system of records, or non-federal records, in order to administer a federal benefit program, personnel system, or payroll system. The CMA documents and evaluates the privacy implications of that linkage. For example, there is a CMA because CMS and the Social Security Administration compare records in order to determine whether individuals qualify for certain income-based health insurance services.

Confidentiality: Preserving authorized restrictions on information access and disclosure.

Conversion: Records currently in paper form will be scanned or otherwise added into a system. (OMB M-03-22 Attachment A provides examples of what system changes could result in a new privacy risk and therefore require an update to an existing PIA. Although this term is the same as that in M-03-22, the definition has been revised for clarity).

Direct personal identifier: Information which is specific to a particular person. A birthday of someone who works for HHS is probably not a direct personal identifier. However, a birthday of someone who works for a particular office within a particular OpDiv may be a direct personal identifier.

Enterprise Performance Lifecycle (EPLC) Framework: An HHS framework to enhance Information Technology (IT) governance through rigorous application of sound investment and project management principles and industry's best practices. The HHS EPLC provides the context for the HHS IT governance process and describes interdependencies between its project management, investment management, and capital planning components. The phases are defined in HHS' Enterprise Performance Life Cycle Framework Overview Document.

Federal Acquisition Regulation (FAR): Primary regulation used by all federal agencies when contracting for supplies and services with appropriated funds.

General Records Schedule (GRS): A NARA-approved records retention schedule that applies to a certain type of records that is common to more than one agency.

HHS Acquisition Regulation (HHSAR): The standard contract clauses in HHS contracts which implement and supplement the FAR.

Implied consent: Individuals implicitly consent to the use or collection of their PII through their behavior. For example, an individual enters a room with a sign on the wall that indicates that he or she may be video-recorded. If that individual remains in the room, he or she consents to being recorded.

Information collection request (ICR): The supporting statement and attachments used to request an OMB Control Number.

Information Sharing Agreement (ISA): A document that establishes the technical requirements that are needed to share and protect electronic information. The purposes and legal requirements will generally be documented in a related MOU.

Integrity: Information is not improperly modified or destroyed and one cannot dispute who provided or modified the information.

Internal Flow or Collection: New types of PII will be added to a system and/or a major change will be made to how a system uses or discloses PII already in a system. (OMB M-03-22 Attachment A provides examples of what system changes could result in a new privacy risk and therefore require an update to an existing PIA. Although this term is the same as that in M-03-22, the definition has been revised for clarity).

Link: Any text, pictures, selectable boxes, and other features that redirect individuals away from the page they are currently viewing.

Machine-readable privacy policy: A document which lists a website's privacy practices in a language that can be read and understood by an internet browser. When placed on a website, the internet browser can automatically compare the website's privacy practices to the visitor's preset preferences and inform the visitor whether or not there are differences between the two.

Memorandum of Understanding (MOU): A document that establishes the terms and conditions for sharing information. It generally includes the reason for the sharing, the authorities that are relevant to the sharing, and the responsibilities of both organizations. The technical requirements will generally be documented in a related ISA.

National Archives and Records Administration (NARA): Responsible for assisting agencies with the creation of, and responsible for approving, retention disposition schedules that authorize the destruction of federal records.

New Interagency Uses: A significantly new use or exchange of PII will occur because HHS will work with one or more other federal agencies to share functions. (OMB M-03-22 Attachment A provides examples of what system changes could result in a new privacy risk and therefore require an update to an existing PIA. Although this term is the same as that in M-03-22, the definition has been revised for clarity).

New Public Access: A system accessed by members of the public will begin using a new user-authenticating technology (e.g., password, digital certificate, biometric identifier). (OMB M-03-22 Attachment A provides examples of what system changes could result in a new privacy risk and therefore require an update to an existing PIA. Although this term is the same as that in M-03-22, the definition has been revised for clarity).

OMB Control Number: A number and expiration date that are required to be displayed on a form that collects information from members of the public if the information collection is subject to the PRA.

Opt-in: Individuals take affirmative action to allow the system to collect or use their PII. In other words, an individual's PII will not be collected and/or used unless that individual grants permission.

Opt-out: Individuals take affirmative action to prevent the collection or use of their PII. In other words, an individual's PII may be used or collected unless that individual specifically says otherwise.

Persistent cookie: A small file placed on a user's computer for a variable length of time when a website is visited. It can be used to gather information about the user and remember the user when he or she returns to the website via the same computer.

Personally Identifiable Information (PII): Defined in OMB M-07-16 Footnote 1 as information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. The types of PII listed in Q15 include some of the types of PII that are commonly collected by HHS systems. Other examples may include:

- Work information including work e-mails and work phone numbers;
- Job titles since many people have a title that is unique to them;
- Home phone numbers and addresses, even if they are publically available;
- Family relationships; and
- E-mails provided when registering for a system.

Physical controls: The physical measures, policies, and procedures designed to protect electronic information systems, buildings, and equipment from unauthorized intrusions, environmental hazards, and natural hazards.

Platform for Privacy Preferences (P3P): The standard vocabulary that should be used to write all machine-readable privacy policies placed on a federal agency's website.

Primary reason for collecting PII: Why a system is collecting and maintaining a particular individual's PII. For example, individual X cannot be enrolled in Medicare without submitting their PII.

Principle of least privilege: Users' system access is limited to the functions and information which is essential to their job functions.

Privacy Act Statement (PAS): The notice that an agency is generally required to provide to an individual when his or her information is solicited for collection into a system of records. It includes a description of:

- How the information may be used;
- Where the information may be disclosed outside the agency;
- The statute or Executive Order giving the agency the authority to request that information;
- Whether the request for information is mandatory or voluntary (see Q26); and
- What may happen to the individual if he or she does not provide part or all of the requested information.

Privacy Impact Assessment (PIA): A methodology that provides information technology (IT) security professionals with a process for assessing whether appropriate privacy policies, procedures, and business practices — as well as applicable administrative, technical, and physical security controls — are implemented to ensure compliance with federal privacy regulations. PIAs are published on HHS.gov and go through a 3 year review process.

Privacy Threshold Analysis (PTA): A PTA is a PIA on a system that does not contain PII or only contains HHS employee information. Please note that direct contractors using HHS credentials are considered HHS employees for the purposes of filling out the PIA form. PTAs remain

internal to HHS and do not have to go through the 3 year review process. A PTA may be updated based on a major change to the system. It is also possible that a change to a system could result in a PTA then meeting the threshold to be a PIA.
Records Control Schedule (RCS): A NARA-approved document which states the duration of time a record should be maintained before it should be destroyed (subject to litigation, audits, and other holds).

Secondary reason for collecting PII: What will a system do with an individuals' PII regardless of whether that particular individual's PII is collected or maintained in the system. For example, using Medicare enrollment information to determine the average age of all Medicare enrollees does not significantly rely on individual X's enrollment.

Security Assessment & Authorization (SA&A): A process, previously called Certification & Accreditation (C&A), which is used by HHS to evaluate the security aspects of each system.

Security Authorization (SA): Also called the Authority to Operate (ATO), this document states that the SA&A has been completed for a system and a senior HHS official will accept the risks of the system if certain security controls are implemented. SAs can be valid for as long as three years.

Session cookie: A small file placed on a user's computer when a website is visited that will only remain until the browser is closed.

Significant System Management Changes: The way a system manages PII will significantly change. For example, a system containing PII that is currently maintained on an HHS server will move to the cloud. (OMB M-03-22 Attachment A provides examples of what system changes could result in a new privacy risk and therefore require an update to an existing PIA. Although this term is the same as that in M-03-22, the definition has been revised for clarity).

Systems of Records Notice (SORN): The Privacy Act requires that a SORN be published in the Federal Register to notify the public about a system of records. HHS SORNs are also available online. Although HHS may revise or create a new SORN, individuals generally have an opportunity to read and provide comments before that occurs. Each SORN will generally describe:

- The types and sources of records in the system of records;
- Who those records are about;
- When, why, and where the records are used within the agency;
- When, why, and where the records may be disclosed outside the agency without the individual's consent;
- How the agency safeguards, stores, retrieves, accesses, retains, and disposes the records;
- How an individual can make notification, access, and correction/amendment requests to the system of records' manager (called a System Manager);
- The legal authorities for maintaining the system of records; and
- If and how the system of records is exempt from certain Privacy Act requirements.

Technical controls: The technology, policies, and procedures used to protect the PII and control access to the PII.

Uniform Resource Locator (URL): A website address such as http://www.hhs.gov/.

Web beacon (i.e., web bug): A small graphic in a webpage or e-mail that allows a server to track a user's online activity or verify if the user has viewed a particular webpage or e-mail.

Web measurement and customization technology: Technology used to remember a user's online interactions with a website in order to measure and analyze usage or customize a user's experience.

Appendix V: Included Authorities Organized by Topic

E-Government Act

- Public Law 107–347, E-Government Act of 2002, Section 208, Privacy provisions
- 44 USC Chapter 35, Subchapter III - Information Security
- OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002
- OMB Memorandum M-05-08, Designation of Senior Agency Officials for Privacy
- HHS OCIO 2009-0002.001, Policy for Privacy Impact Assessment (PIA)
- HHS-OCIO-2011-0003, Revisions to the HHS-OCIO Policy for Information Systems Security and Privacy
- HHS-OCIO-2013-0002, HHS Information Sharing Environment (ISE) Privacy Policy
- HHS Standard 2008-0006.001S, HHS Standard for FISMA Inventory Management
- HHS Memo for Change of Review Period for Privacy Impact Assessments (on intranet)

Privacy Act

- PL 93–579, Approved December 31, 1974 (88 Stat. 1896)
- 5 USC 552a, Records maintained on individuals i.e., The Privacy Act of 1974, as amended
- 45 CFR 5b, Privacy Act Regulations
- OMB Circular No. A-130 Revised, Management of Federal Information Resources
- OMB M-01-05, Guidance on Inter-Agency Sharing of Personal Data - Protecting Personal Privacy
- OMB Privacy Act Implementation: Guidelines and Responsibilities, 40 FR 28962
- The Overview of the Privacy Act of 1974 as prepared by the Department of Justice's Office of Privacy and Civil Liberties
- The Federal Register Document Drafting Handbook

Privacy & Websites

- OMB M-99-18, Privacy Policies on Federal Web Sites
- OMB Memorandum M-10-22, Guidance for Online Use of Web Measurement and Customization Technologies
- OMB Memorandum M-10-23, Guidance for Agency Use of Third-Party Websites and Applications
- HHS Memorandum, Implementation of OMB M-10-22 and M-10-23
- HHS-OCIO-2010-0001 Policy for Machine-Readable Privacy Policies
- HHS Machine-Readable Privacy Policy Guide and the Privacy Policy Machine Readable Training (PDF on intranet)

Privacy & Contracts

- Federal Acquisition Regulation, issued March 2005 by the General Services Administration, Department of Defense, National Aeronautics and Space Administration
- HHS Acquisition Regulation

Children's Online Privacy Protection Rule (COPPA)

- 5 USC 6501–6505, Children's Online Privacy Protection Act of 1998
- 15 USC Chapter 91, Children's Online Privacy Protection
- 16 CFR Part 312, Children's Online Privacy Protection Rule: Final Rule Amendments to Clarify the Scope of the Rule and Strengthen its Protections for Children's Personal Information

NIST Publications

- NIST FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems
- NIST FIPS Publication 200, Minimum Security Requirement for Federal Information and Information Systems
- NIST Special Publication 800-37 Revision 1, Information Security
- NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations
- NIST Special Publication 800-100, Information Security Handbook: A Guide for Managers
- NIST 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information

Privacy & Breach Response:

- OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information
- HHS Response Plan to M0716 070919: Response to Attachment 1: Safeguarding Against the Breach of Personally Identifiable Information (PII)

Records Management / Paperwork Reduction Act

- 44 USC Chapter 33, Disposal of Records
- 44 USC Chapter 35, Subchapter I - Federal Information Policy
- 36 CFR 1228 - Disposition of Federal Records
- Parts of the CFR which affect NARA
- NARA's Records Management Publications
- HHS Guidance for completing an ICR

Social Security Number Usage:

- E.O. 9397, Numbering System for Federal Accounts Relating to Individual Persons
- E.O. 13478, Amendments To Executive Order 9397 Relating To Federal Agency Use of Social Security Numbers

Other:

- 5 USC 301, Departmental regulations
- HIPAA Security Rule
- OMB Letter to GAO dated 6/8/07 (copy included in GAO-07-752)