Privacy Impact Assessments

Enterprise Privacy Office

March 2016

admin

THE SOUTH CAROLINA DEPARTMENT *of* ADMINISTRATION

Presentation Objectives

- Describe the purpose, scope and benefits of conducting a Privacy Threshold Analysis/Privacy Impact Assessment (PTA/PIA).
- Review the PTA/PIA template questions.
- Provide tips on implementing the PTA/PIA process.

admin
THE SOUTH CAROLINA
DEPARTMENT of ADMINISTRATION

admin
THE SOUTH CAROLINA
DEPARTMENT *of* ADMINISTRATION

Requirement

- SCDIS-200 Information Security and Privacy Standard Control 12.400, Data Protection and Privacy

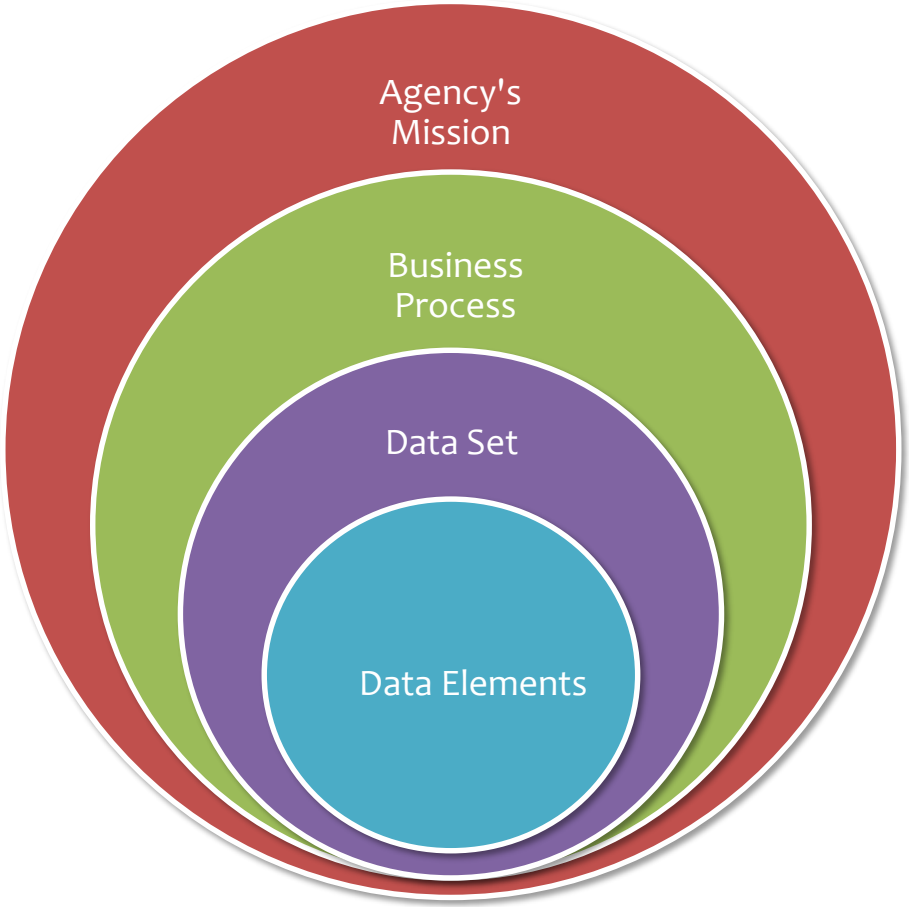
"Each agency must ensure the interests of data subjects are appropriately protected."

admin
THE SOUTH CAROLINA DEPARTMENT of ADMINISTRATION

What is the purpose of the PTA/PIA?

- Provides a comprehensive analysis of privacy risk in the Agency's business process:
  - The business process can include both electronic and paper based records.
  - Completing Data Classification prior to beginning the PTA/PIA process is beneficial.

Scope of Analyses



admin
THE SOUTH CAROLINA DEPARTMENT of ADMINISTRATION

Benefits of the PTA/PIA

- Validates the use of PII in business processes.
- Assesses privacy risks.
- Evaluates current privacy protections and determines mitigation actions.

What is a PTA?

- Documents whether the business process collects, uses, processes, shares, retains, or disposes of PII:
  - If no PII is identified, no further privacy risk analysis is warranted.
  - If PII is identified, a full Privacy Impact Assessment (PIA) is needed.

admin
THE SOUTH CAROLINA DEPARTMENT of ADMINISTRATION

What is a PIA?

- Analyzes how PII is handled:
  - Ensures information handling conforms to applicable legal, regulatory, and policy requirements.
  - Determines the risks and effects of collecting, maintaining, and disseminating information in identifiable form.
  - Examines and evaluates protections and alternative processes for handling information to mitigate potential privacy risks.

The PTA/PIA Process

admin
THE SOUTH CAROLINA
DEPARTMENT of ADMINISTRATION

PTA/PIA Guide

- PTA/PIA Guidance document is used to assist Agencies with completing the PTA/PIA.
- The guide is divided into four sections:
  - Guidance on Completing the PTA/PIA
  - Appendix A: Instructions for Completing
  - Appendix B: PTA/PIA Template
  - Appendix C: Findings and Mitigation Plan

admin
THE SOUTH CAROLINA DEPARTMENT of ADMINISTRATION

Phases of the PTA/PIA Process

Preparation

- Data classification
- Assessing the data elements within the business process
- Assessing the location

PTA

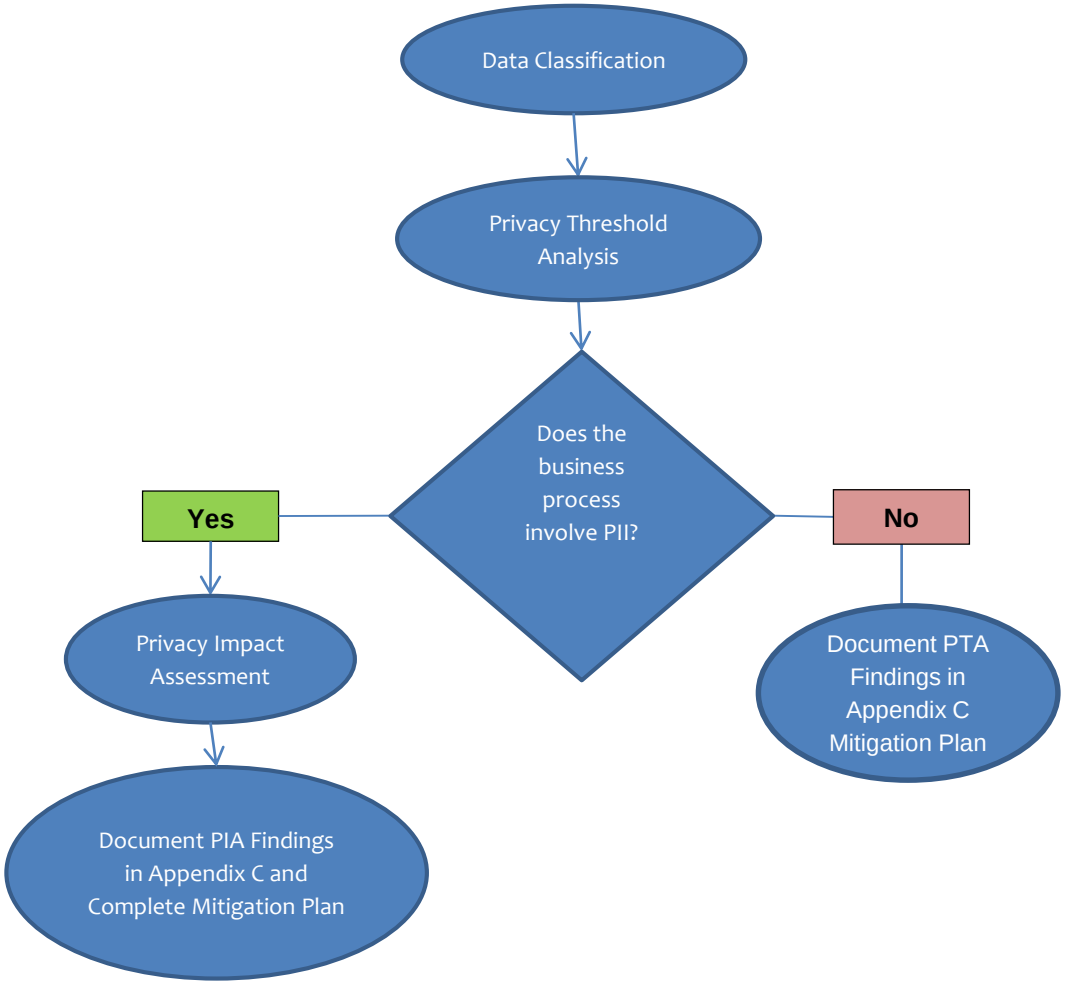
- Review to determine the collection, retention, sharing, use, or disposal of PII
- PTA is used to determine whether or not PII is involved in the business process
- If no PII, no further action is needed
- If PII, a PIA is required

PIA

- Analyze how PII is handled during a specific business process
- To include how the information is collected, stored, shared, used, and / or retained
- Once the PIA is complete, evaluate risks

admin
THE SOUTH CAROLINA DEPARTMENT of ADMINISTRATION

PTA/PIA Process



admin
THE SOUTH CAROLINA DEPARTMENT of ADMINISTRATION

Privacy Threshold Analysis

admin
THE SOUTH CAROLINA
DEPARTMENT of ADMINISTRATION

PTA: Section 1.0

Section 1.0 General Information

Business Process:			
Agency Name		**PTA/PIA #**	<Enter PTA/PIA# # assigned by the Agency Privacy Liaison or if this is an update to existing PTA/PIA, enter the original PTA/PIA #>
System Owner			
Agency Privacy Liaison:			
New PTA/PIA?	☐ Yes ☐ No, update to an existing PTA/PIA		
If this is an update to an existing PIA, include the initial PTA/PIA Number and a reason for the update:			

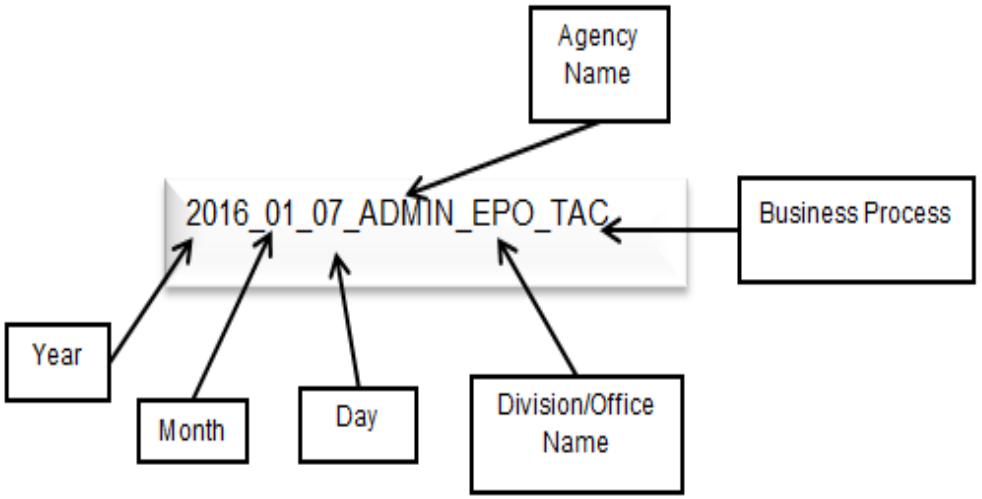
Section 1.0 General Information: This section asks for the general information related to the business process. The name of the Agency, System Owner, and Agency Privacy Liaison.

The PIA/PTA Number is assigned by the Agency Privacy Liaison. (See next slide for specific example.) The PTA/PIA# is used to track the PTA/PIA throughout the lifecycle of the business process and should be used if the PTA/PIA is updated.

admin
THE SOUTH CAROLINA DEPARTMENT of ADMINISTRATION

How to write the PTA/PIA Number

Year/Month/Day: Year, month and day the PTA/PIA form was submitted to the Agency Privacy Liaison.
Agency Name-Identify the specific Agency abbreviation.
Division/Office Name- Identify the specific division/office name responsible for the business process.
Business Process- Use only the abbreviation of the business process. For Example Time and Compliance (TAC)



admin
THE SOUTH CAROLINA DEPARTMENT of ADMINISTRATION

PTA: Section 2.0

Section 2.0 Overview

2.1 Provide a brief overview of the business purpose:

Briefly describe the data set, including:

- *The business purpose of the Agency and how the Agency's data elements support the program and Agency mission;*
- *A general description of the information in the data set's data records,*
- *Whether the data elements are paper-based, electronic or a hybrid.*

Section 2.0 Overview

Provide a brief description of the business process, provide as much information as possible about the information that is processed to ensure the Agency Privacy Liaison has a clear understanding of the data.

admin
THE SOUTH CAROLINA DEPARTMENT of ADMINISTRATION

PTA: Section 3.0

Section 3.0 Data Characteristics

3.1 What Personally Identifiable Information (PII), contained in the Agency data set, is collected, used, retained, or shared? *(Check all that apply.)*			
☐ Social Security Number	☐ Name	☐ Spouse Information	☐ Personal Cell Phone
☐ Driver's License Number	☐ Date of Birth	☐ Security Clearance	☐ Office Phone Number
☐ Passport Number	☐ Place of Birth	☐ Law Enforcement	☐ Office Direct Phone Number
☐ Personal Credit or Debit Card Number	☐ Home Address	☐ Emergency Contact	☐ Work Email Address
☐ Personal Financial Information	☐ Maiden Name	☐ Military Status/Service	☐ Biometrics
☐ Taxpayer ID	☐ Gender	☐ Employment Information	☐ User ID
☐ Employee ID	☐ Age	☐ Education Information	☐ IP Address
☐ Health Insurance Beneficiary	☐ Race/Ethnicity	☐ Other Names Used	☐ MAC Address
☐ Vehicle License Plate	☐ Personal Email Address	☐ Salary	☐ Occupation
☐ State Identification	☐ Religion	☐ Work Address	
☐ Mother's Maiden Name	☐ Medical Information	☐ Job Title	
☐ Other:			

3.2 What is the source of the PII collected? (Check all that apply.)				
☐ Individual	☐ SC State Agency	☐ Federal Agency	☐ County Agency	☐ Local Agency
☐ Other				

3.3 How is the information collected for this business process? (Check all that apply.)				
☐ Paper Format	☐ In-Person Interview	☐ Facsimile	☐ Telephone Interview	☐ Email
☐ Website	☐ Interagency Sharing	☐ Other		

admin
THE SOUTH CAROLINA DEPARTMENT of ADMINISTRATION

Agency Privacy Liaison Review

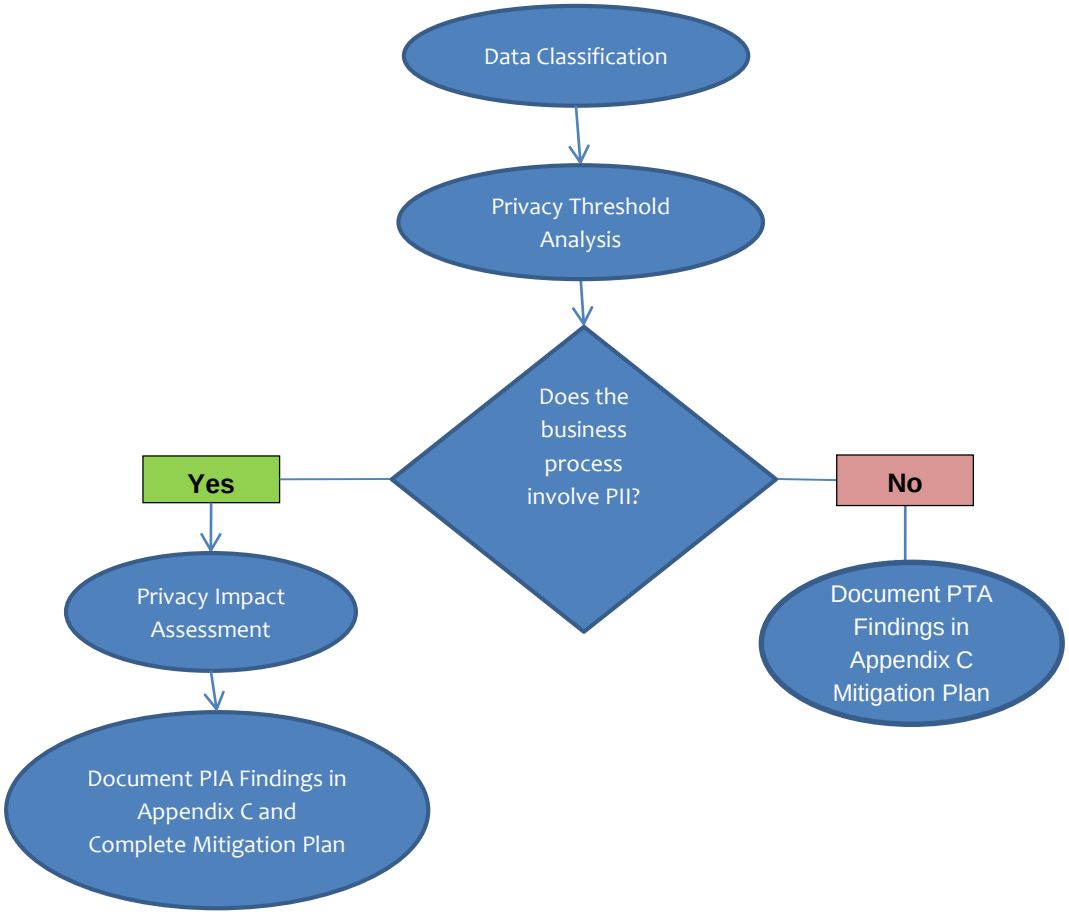
STOP **Please stop here, and submit this form to the Agency Privacy Liaison.**

Agency Privacy Liaison:	
Does the business process/system contain PII?	Yes ☐ (If Yes, complete the PIA) No ☐
Comments:	

Agency Privacy Liaison will review the PTA and determine whether a full PIA is needed.

admin
THE SOUTH CAROLINA DEPARTMENT of ADMINISTRATION

PTA/PIA Process



admin
THE SOUTH CAROLINA DEPARTMENT of ADMINISTRATION

Privacy Impact Assessment

admin
THE SOUTH CAROLINA
DEPARTMENT of ADMINISTRATION

Supporting Documentation

- Supporting documentation will assist Privacy Liaisons with understanding fully the business process.
- Ensure the following documents are available:
  - Data Flow mapping of the business process
  - Data Collection Tools
  - Data Sharing Agreements

admin
THE SOUTH CAROLINA
DEPARTMENT of ADMINISTRATION

PIA

- Questions in the PIA address the seven privacy principles:
  - Notice and Transparency
  - Use and Disclosure Limitation
  - Individual Participation, Access, and Redress
  - Data Minimization and Retention
  - Data Quality and Integrity
  - Security
  - Accountability and Auditing

admin
THE SOUTH CAROLINA
DEPARTMENT of ADMINISTRATION

Notice and Transparency

- Provide notice to the individuals about the personal information collected; how the information will be used and shared.
- Communicate in plain language and is accessible to the individual.

Reference PIA Section 5.0

admin
THE SOUTH CAROLINA
DEPARTMENT *of* ADMINISTRATION

Notice and Transparency

Section 5.0 Notice to Individuals to Decline/Consent Use

5.1 How is notice provided to the individual prior to the collection of information? If notice is not provided, explain why. Include the links to any web-based Privacy Policy or Notice. *Providing notice is the method by which an individual is informed of how his or her information will be used. Notice is provided prior to the collection of the individual's information. Please refer to the specific federal and/or State law, regulation, and/or Agency policy that applies to the collection of information from individuals.*

Describe the process used to provide individuals with notice prior to the collection of their information. This could be as simple as privacy notice on the top of the information collection or the privacy notice on a website.

admin
THE SOUTH CAROLINA
DEPARTMENT of ADMINISTRATION

Notice and Transparency

5.2 Are individuals allowed to decline to provide information?
☐ Yes (Complete Question 5.3) ☐ No (Complete Question 5.4)

5.3 If individuals ARE allowed to decline to provide information, how are any resulting consequences, e.g., the State's inability to provide the service, explained to the individual?

5.4 If individuals are NOT allowed to decline to provide information, is notice of the collection of information provided to the individual? If notice is not provided, please provide detailed justification.

5.5 Are individuals informed of their right to consent to particular uses of the information (if applicable)? If so, how does the individual exercise that right?

admin
THE SOUTH CAROLINA
DEPARTMENT of ADMINISTRATION

Use and Disclosure Limitation

- Use and disclose the individual's information only as indicated in the notification provided.
- Using an individual's information outside of the notice requires explicit consent, except in certain instances—such as law enforcement.

Reference PIA Sections 1.0, 2.0, and 4.0

admin
THE SOUTH CAROLINA
DEPARTMENT *of* ADMINISTRATION

Use and Disclosure Limitation

Section 1.0 Data Collection

1.1 What is the source of the PII collected for this business process? (Check all that apply.) *This information can be copied from the PTA.*				
☐ Individual	☐ SC State Agency	☐ Federal Agency	☐ County Agency	☐ Local Agency
☐ Other				
Describe:				

1.2 How is the information collected by the business process? (Check all that apply.) *This information may be copied from the PTA.*				
☐ Paper Form	☐ In-person Interview	☐ Facsimile	☐ Telephone Interview	☐ Email
☐ Website	☐ Interagency Sharing	☐ Other:		
Describe:				

admin
THE SOUTH CAROLINA DEPARTMENT of ADMINISTRATION

Use and Disclosure Limitation

1.3 What is the purpose for which the PII is being collected, used, shared, or retained? *Describe why the particular PII collected, used, shared, or retained in the business process is necessary to the program or Agency mission.*

1.5 What is the legal authority for the collection of information? Provide the specific citations. *Examples may include federal statutes, State law, and/or regulations.*

admin
THE SOUTH CAROLINA
DEPARTMENT of ADMINISTRATION

Use and Disclosure Limitation

1.6 What are the regulatory compliance privacy requirements?		
☐ HIPAA-HITECH	☐ GLBA	☐ CJIS
☐ IRS Publication 1075	☐ FERPA	☐ PCI-DSS
☐ Other (Provide the citation and a brief description)		

Section 2.0 Data Use

2.1 How is the information in the data sets used to support the Agency?

admin
THE SOUTH CAROLINA
DEPARTMENT of ADMINISTRATION

Use and Disclosure Limitation

Section 4.0 Data Sharing

4.1 Describe data sharing with State of South Carolina Government entities.

State of South Carolina Government Entity	*Purpose for which information is shared*	*Specific information types that are shared*	*Method of transmittal or disclosure*	*Safeguards for data transmittal and disclosure*
EX. MyFellow Entity	**Information is shared with MyFellow Entity A for mandatory reporting under law JKL.**	**Name, Work Address, Work Telephone Number, and Work Email Address**	**Weekly Secure File Transfer Protocol**	**Information shared with the MyFellow Entity is sent via a file transfer**

4.3 Describe data sharing with the non-State of South Carolina Government entities.

Non-State of South Carolina Government Entity	*Purpose for which information is shared*	*Specific information types that are shared*	*Method of transmittal or disclosure*	*Safeguards for data transmittal and disclosure*
EX: Company Q	**Insurance verification**	**Name, Personal Address, Social Security Number**	**Data is transferred via a secure file transfer every 3 months.**	**Data is sent via a secure one way file transfer using File Transfer Protocol.**

4.2 What agreements, and other types of documentation, are in place, which establish parameters around the internal data sharing listed above, and how frequently are these documents reviewed?

Examples: Memorandum of Agreement or Memorandum of Understanding (MOA/MOU) between Agency and Entity is reviewed annually. Contract XYZ is reviewed every three years.

Individual Participation, Access, and Redress

- Provide individuals with the opportunity to consent to the collection, use, or disclosure of personal information.
- Allow individuals the procedures to access information being held about them, make corrections or update that information, and the point of contacts for further questions.

Reference PIA Section 6.0

admin
THE SOUTH CAROLINA
DEPARTMENT *of* ADMINISTRATION

Individual Participation, Access, and Redress

Section 6.0 Individual Requests for Access, Redress, and/or Correction

6.1 What are the procedures that allow an individual to request access and/or to correct the information the Agency has collected regarding his or her information? How are individuals informed of this process?

6.2 Is there a way for an individual, who is dissatisfied with the Agency's initial response to his or her request for data access or correction, to ask for a review of the decision? If so, describe the process.

admin
THE SOUTH CAROLINA
DEPARTMENT of ADMINISTRATION

Data Minimization and Retention

- Ensuring the business process collects only the minimum amount of information necessary perform the official task.
- The retained information is collected and used for as long as necessary to fulfill the purpose for which it was requested.

Reference PIA Section 3.0

admin
THE SOUTH CAROLINA DEPARTMENT of ADMINISTRATION

Data Minimization and Retention

Section 3.0 Data Retention

3.1 What information is retained by the Agency? *This may include any third party organizations contracted to retain information for the Agency.*

3.2 How long is information retained, and under what retention schedule? *Describe any exceptions to the retention schedule. Consult your Agency Records Officer or Agency General Counsel for advice regarding information retention schedules.*

admin
THE SOUTH CAROLINA
DEPARTMENT of ADMINISTRATION

Data Minimization and Retention

3.3 What are the Agency's procedures for the disposal of information at the end of the retention period?

Describe policies and procedures for how PII that is no longer relevant and necessary is purged. This information may be obtained from the Agency Records Officer or Agency General Counsel.

Example: Paper records are shredded, in accordance with DIS Information Security and Privacy Standards, by a vendor under contract with the State. The disposal is documented by way of a certificate of destruction.

3.4 Where are the procedures documented? How are disposal procedures audited for compliance?

3.5 Where is information maintained or stored?

Example: XYZ Agency currently has a contract with VendorStore USA, Inc. The data is stored on servers located in a secure facility in Charlotte, NC.

Example: XYZ Agency currently has an (ISA/MOU) with the Division of Technology (DT). The servers are located at the Broad River Road Facility.

admin
THE SOUTH CAROLINA DEPARTMENT of ADMINISTRATION

Data Quality and Integrity

- Establish policies and procedures to ensure, to the greatest extent practicable, that data is accurate, complete, and up-to-date.

Reference PIA Question 1.4

admin
THE SOUTH CAROLINA
DEPARTMENT *of* ADMINISTRATION

Data Quality and Integrity

1.4 How is the information checked for accuracy? *For example, is the information checked for accuracy through comparison with another source? Are individuals required to revalidate information?*

Checking for accuracy can include reviewing audit logs, error codes in electronic database forms, or comparing information from other sources.

admin
THE SOUTH CAROLINA DEPARTMENT of ADMINISTRATION

Security

- Establishing the appropriate levels of administrative, technical, and operational controls,
- Ensuring the safeguards preserve the privacy, confidentiality, integrity, and accessibility of personal information.

Reference PIA Section 7.0

admin
THE SOUTH CAROLINA DEPARTMENT of ADMINISTRATION

Security

Section 7.0 Access Privileges and Security

7.1 What criteria are in place to determine which users or roles may access the Agency data records? Where are the procedures for requesting and modifying access privileges documented?

7.3 How are persons, who are given access to this data set, made aware of privacy safeguards?

Tip: Examine the Access Control Policy or User Guide (7.1 & 7.3)

7.2 Do contractors have access to the Agency data records? If yes, describe privacy-related safeguards and requirements built into the contract language.
Examples of privacy safeguards may include: certification of privacy training prior to data access; non-disclosure or confidentiality agreements; background checks; and data breach reporting and notification responsibilities, etc.

Tip: Ensure the security & privacy requirements have been included in contracts.

admin
THE SOUTH CAROLINA DEPARTMENT of ADMINISTRATION

Security

7.4 Have the appropriate controls been implemented in accordance with the State Information Security Program (SC DIS 200 Standard 1.400)? Has the designated Agency manager documented his/her decision to accept any identified risks (SC DIS Control 4.205)?

7.5 What physical, administrative, and technical controls are in place to protect the data from unauthorized access and misuse? *Please describe the Physical, Technical, and Administrative Controls currently in place to account for and secure the PII.*

Work with Agency Security Liaisons to document and ensure the appropriate controls have been identified and assess, and ensure the agency has identified a manager to accept any risks.

Accountability and Auditing

- Establish policies and procedures that assign information protection roles and responsibilities, and institute processes for evaluating, compliance, effectiveness, and improvement.
- The Accountability and Auditing Privacy principles covers multiple questions.

Accountability and Auditing

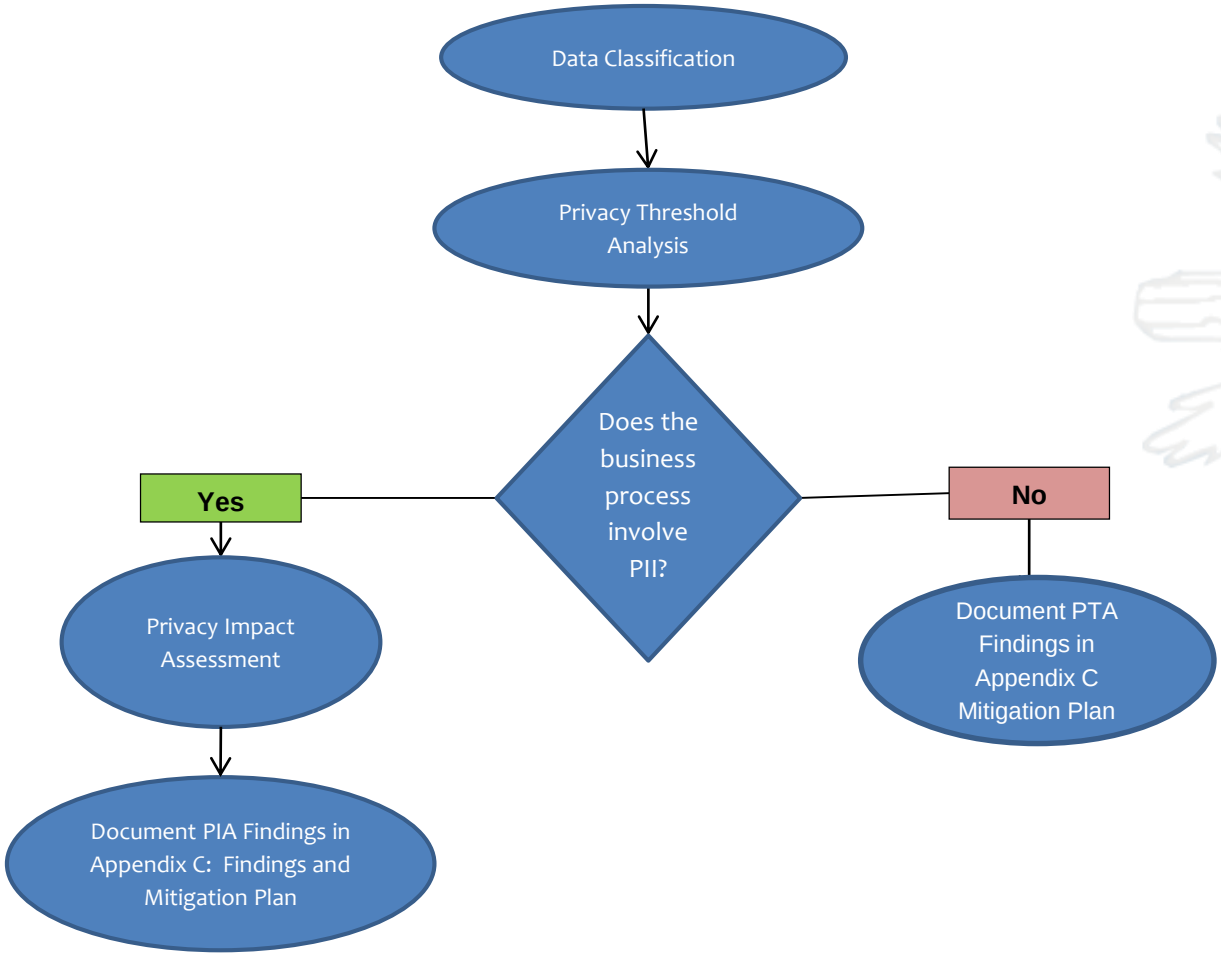
1.4 How is the information checked for accuracy? *For example, is the information checked for accuracy through comparison with another source? Are individuals required to revalidate information?*

7.4 Have the appropriate controls been implemented in accordance with the State Information Security Program (SC DIS 200 Standard 1.400)? Has the designated Agency manager documented his/her decision to accept any identified risks (SC DIS Control 4.205)?

7.5 What physical, administrative, and technical controls are in place to protect the data from unauthorized access and misuse? *Please describe the Physical, Technical, and Administrative Controls currently in place to account for and secure the PII.*

admin
THE SOUTH CAROLINA
DEPARTMENT of ADMINISTRATION

PTA/PIA Process



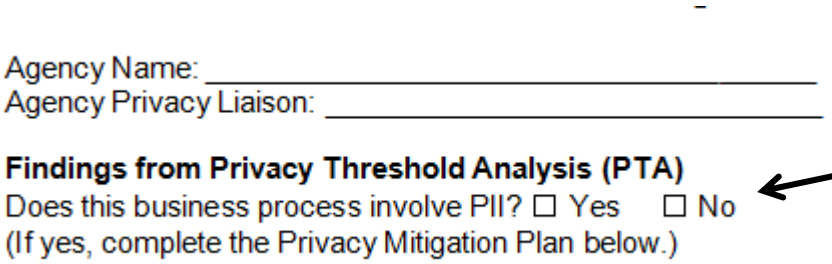
admin
THE SOUTH CAROLINA DEPARTMENT of ADMINISTRATION

Findings and Mitigation Plan

admin
THE SOUTH CAROLINA
DEPARTMENT of ADMINISTRATION

Findings and Mitigation Plan

- PTA/PIA Findings and Mitigation Plan is used to assess privacy risk identified during the PIA.
- If no PII is found, answer the first question "No" and no additional information is needed.



Agency Name: _____
Agency Privacy Liaison: _____

Findings from Privacy Threshold Analysis (PTA)
Does this business process involve PII? ☐ Yes ☐ No
(If yes, complete the Privacy Mitigation Plan below.)

If no PII is found in the business process- check the box "No". No further information is needed.

admin
THE SOUTH CAROLINA DEPARTMENT of ADMINISTRATION

Findings and Mitigation Plan

- If the business process has PII, complete the Privacy Mitigation Plan to document each risk identified during the assessment.
- Provide a brief description of each privacy risk

Privacy Mitigation Plan						
Risk #	Description of Privacy Risk	Planned Mitigation Action	Person Responsible for Mitigation Action	Projected Completion Date	Status*	Comments
1						
2						
3						
4						
5						

***Status:** **OT = On Target** **C = Closed** **D = Delayed**

admin
THE SOUTH CAROLINA DEPARTMENT of ADMINISTRATION

Findings and Mitigation Plan

Privacy Mitigation Plan						
Risk #	**Description of Privacy Risk**	**Planned Mitigation Action**	**Person Responsible for Mitigation Action**	**Projected Completion Date**	**Status***	**Comments**
1.	Unsure of legal authority to use the data collected.	Seek legal guidance from the Agency Counsel; review privacy requirements to ensure collection is necessary.	Jane Doe	12/16/2016	OT	
2.	Users storing PII in unlocked/unsecured file cabinets	Provide privacy training for users; Files will be moved to a secure file cabinet/ storage area	Star Fish	06/30/2016	OT	
3.	Unsure of retention and destruction policies related to the business process	Contact Archivist for additional information	Jane Doe	03/15/2016	C	3/2/2016- Spoke to Archivist or Agency's Records Office provide a description of the records collected for the business process. Received updated retention schedule from Archivist.
4.						
5.						

***Status:** **OT = On Target** **C = Closed** **D = Delayed**

admin
THE SOUTH CAROLINA DEPARTMENT of ADMINISTRATION

Tips

- Responses to PIA questions should concise, yet detailed enough to give a full picture of the data posture.
- Assemble a team of stakeholders to help with the completion of the PTA/PIA.
- Consider starting with a smaller process. This will allow you and your team to gain a clearer understanding the PIA process before tackling a larger process.

admin
THE SOUTH CAROLINA
DEPARTMENT of ADMINISTRATION