Privacy Threshold Analysis (PTA) and Privacy Impact Assessment (PIA)

Statewide Procedure

Version 1.0

August 14, 2026

Document Information

Revision History

Date	Version	New or Revised Requirement	Description	Author
Aug. 14, 2026	1.0	New	Standard Creation	Martha K. Wewer

Document Details

Department Name	Office of Privacy and Data Protection
Owner	Martha K. Wewer
Title	PTA and PIA Procedure
Publication Date	Aug. 14, 2026
Next Revision	Aug. 14, 2026
Document Type	
Document Number	
Version	1.0

Table of Contents

Purpose

The Office of Privacy and Data Protection (OPDP), within the N.C. Department of Information Technology, is tasked with protecting state data.

To accomplish data protection while protecting the privacy of constituents, employees, and other data entrusted to the state, Privacy Threshold Analysis (PTAs) and Privacy Impact Assessments (PIAs) are required to identify, evaluate, and mitigate privacy risks throughout the data lifecycle of a program, project, system, or technology involving state data.

This Procedure, issued under the Statewide Privacy and Data Protection Policy, establishes the requirements and process for completing and submitting PTAs and PIAs to OPDP for review and approval.

Content Lead

N.C. Department of Information Technology, Office of Privacy and Data Protection

Scope

This Procedure applies to state agencies, subject to the Statewide Privacy and Data Protection Policy, that create, collect, use, maintain, share, or dispose of state data.

Procedure

Privacy Threshold Analysis (PTAs)

State agencies are required to complete a Privacy Threshold Analysis (PTA) at project initiation for any of the following:

- Launch of a new system, application, or database
- Major enhancements or material changes (defined as “a change that impacts the collection, use, disclosure, storage, or processing of state data”) to existing systems
- Introduction of new data elements or collection methods
- Use of AI, automation, analytics, or third-party services or tools that process state data
- Migration of systems to a cloud environment
- Integration between existing systems

In short, a PTA is required whenever a new tool, project, or system is introduced or an existing tool, project, or system undergoes a material change affecting the collection, use, disclosure, storage, or processing of state data.

A PTA may collect information (if known at the time of submission) such as:

- A general description of the IT system, tool, technology, program, pilot project, information-sharing arrangement, the business purpose, the systems involved, and whether the project involves a contractor or third party
- Whether the project collects, creates, receives, or uses personal information
- Whether the project involves federally regulated data
- Whether the project requires new data elements not currently collected by the existing tool, system, application, or database
- Whether data is collected directly from individuals or indirectly from another system or agency

- Data location and who has access
- Data retention period

Based on the completed PTA, OPDP will determine one of the following outcomes:

- No further review is required because:
    - No personal information is involved. The data classification in accordance with the Statewide Data Classification and Handling Policy is Public.
    - The project uses existing data systems without changes
    - No external data sharing has been introduced.
- A Privacy Impact Assessment (PIA) is required because:
    - Personal information is collected. The data classification is set to Internal, Confidential, or Restricted.
    - New storage, sharing, or collection practices are introduced.
    - There is use of artificial intelligence tools with data classified as Internal, Confidential, or Restricted.
    - There is a recognized risk to state data that requires additional review.

All agencies incorporating a technology or system must begin the compliance process with a PTA, as it:

- Serves as the official determination by OPDP as to whether a technology or system's intended use has privacy implications
- Is required by the Statewide Information Security Manual (CA-3 Information Exchange; RA-2 Security Categorization)

PTAs must be reviewed and renewed annually or prior to a material change in the data, tool, project, or system.

PTAs must be:

- Completed by the Program Manager, Project Manager, or Agency Privacy Liaison
- Submitted to the Agency Privacy Liaison for approval
- Submitted by the Agency Privacy Liaison to OPDP for review and approval

Please see the following guidance documents:

- PTA & PIA User Guide for State Agencies
- PTA & PIA User Guide for NCDIT Employees

Privacy Impact Assessments (PIAs)

The PIA process is managed by OPDP.

PIAs are tools used to identify, assess, and mitigate privacy risks associated with the collection, use, storage, and sharing of state data.

A PIA is required when the completed PTA identifies privacy risks requiring additional assessment. A PIA supports the state's goals of data protection by ensuring and documenting that:

- State data is handled in compliance with legal, regulatory, and contractual obligations
- Privacy risks are identified early and addressed consistently across agencies

- Classification, security and privacy controls, and data governance practices are appropriately aligned
- Projects meet statewide expectations for responsible and transparent data use

A PIA may collect information (if known at the time of submission) such as:

- Types of data collected or processed (e.g., PII, PHI, financial, education, geospatial, criminal justice)
- Classification level (per the Statewide Data Classification and Handling Policy)
- Whether the data involves minors, vulnerable populations, or high-risk groups
- Source of data (direct collection, existing systems, vendors, interagency feeds)
- Collection methods, storage locations, access control, data sharing, retention schedules, and disposal practices
- The purpose for the data elements being collected – only the necessary amount or types of data is being collected and no more
- Any third party in receipt of data
- Applicable administrative controls such as training, monitoring and policies

Similar to the PTA, a PIA must be:

- Completed by the Program Manager, Project Manager, or Agency Privacy Liaison
- Submitted to the Privacy Liaison for review and approval
- Submitted by the Agency Privacy Liaison to OPDP for review and approval

A PIA should be completed before implementation of the system, project, or material change whenever practicable. This will aid in identifying privacy risks so they may be addressed prior to the processing of state data.

To ensure risk management is a continuous practice, each agency must also maintain and review at least annually a Data Risk Register for any system processing Confidential or Restricted data. (For guidance on creating and maintaining a Data Risk Register, please contact the Office of Privacy and Data Protection at opdp@nc.gov.

PIAs must be reviewed and renewed annually or whenever there is a material change in the data, tool, project, or system.

Additional Requirements for AI Systems

For tools or systems using artificial intelligence (AI), state agencies should be prepared, if requested, to submit a completed AI-Use Case Risk Profile with the PTA/PIA. (The AI-Use Case Risk Profile can be found in the AI Working Group Starter Pack.)

As required by AI policy, each agency must maintain an AI Inventory. AI Tools collecting, processing or sharing Confidential or Restricted Data can be noted on the AI Inventory or on the Data Risk Register.

Review, Approval, and Publication of Assessments

OPDP will review PTAs and PIAs for completeness, proper data classification (based on the data elements identified), regulatory compliance, privacy controls enabled for data protection, and data sharing.

Tools, applications, or systems with multiple types of data will be classified at the highest data classification level. For example, if a system has Protected Health Information (Restricted) as well as

agency policies and procedures (Internal), the system will be classified as Restricted for the purposes of the PIA.

Agencies should identify all data elements when completing the PTA and PIA.

PTAs and PIAs that are complete, specific, and detailed will result in quicker review. OPDP is always available for consultation on the appropriate way to complete a PTA or PIA.

Agency PTAs and PIAs will not be visible to other agencies.

However, to promote visibility into technology adoption, to leverage other agency tools, and to inform potential statewide vendor engagement and procurement opportunities, OPDP will produce:

- Quarterly metrics regarding the number of PTAs and PIAs approved or returned for comment
- Average review timeline
- A list of approved tools, applications or systems with agency name

Roles and Responsibilities

- **Office of Privacy and Data Protection** – Reviews, assesses and approves PTAs and PIAs, provides guidance on the PTA/PIA process, and maintains statewide metrics
- **Program or Project Manager** – Initiates and completes PTA and/or PIA, and, where applicable, the AI Use Case Risk Profile
- **Privacy Liaison (or Privacy Point of Contact)** – Reviews and approves PTA and/or PIAs prior to submission to OPDP and coordinates submission of the AI Use Case Risk Profile, when applicable, and oversees maintenance of the Agency's Data Risk Register as required.

Role	Responsibility
Office of Privacy and Data Protection	• Reviews, assesses and approves PTAs and PIAs • Provides guidance on the PTA/PIA process • Maintains statewide metrics
Program or Project Manager	• Initiates and completes PTA and/or PIA • Initiates and completes the AI Use Case Risk Profile, when applicable
Privacy Liaison (or Privacy Point of Contact)	• Reviews and approves PTA and/or PIAs prior to submission to OPDP • Coordinates submission of the AI Use Case Risk Profile, when applicable • Oversees maintenance of the agency's Data Risk Register, as required

Regulations and Applicable Laws

Statewide Data Classification and Handling Policy
Statewide Information Security Manual

Enforcement

Violations of this Procedure or failure to implement its requirements may result in disciplinary action, up to and including termination, civil litigation, and/or criminal prosecution, as applicable.

Procedure Review Cycle

This Procedure, as part of the Privacy and Data Protection Policy, will undergo a periodic review at annual intervals, or as changes are required. Updates to the Procedure will be determined based upon the nature of the Procedure and requirements driven by need.

Any identified changes, or outdated information within the Procedure will be addressed promptly. This may involve revisions, additions, or removals as needed to ensure that this Procedure remains current, relevant, and aligned with the Statewide Privacy and Data Protection Policy.

The following roles provide leadership and management over this Procedure in accordance with the NCDIT Policy Management Policy:

- Statewide Chief Privacy Officer
- Statewide Chief Information Security Officer
- N.C. Department of Information Technology; Office of the General Counsel

Definitions

Personal Information

Under N.C.G.S. 75-61(10)), state law, personal information is a person's first name or first initial and last name in combination with other identifying information

Identifying information is defined under N.C.G.S. 14-113.20(b) as:

- Social Security or employer taxpayer identification numbers
- Driver's license, state identification card, or passport numbers
- Checking account numbers
- Savings account numbers
- Credit card numbers
- Debit card numbers
- Personal Identification (PIN) Code as defined in G.S. 14-113.8(6)
- Electronic identification numbers, electronic mail names or addresses, internet account numbers, or internet identification names
- Digital signatures
- Any other numbers or information that can be used to access a person's financial resources
- Biometric data
- Fingerprints
- Passwords
- Parent's legal surname prior to marriage. (N.C.G.S. 14-113.20(b), N.C.G.S. 132-1.10)

Please note: Personal information does not include publicly available directories containing information an individual has voluntarily consented to have publicly disseminated or listed, including name, address, and telephone number, and does not include information made lawfully available to the general public from federal, state, or local government records. (See N.C.G.S. 75-61(10)).

Program

A specific set of ordered operations for a computing device to perform.

Project or Program Manager

The senior person responsible for an entire project.

System

An assembly of components (hardware, software, procedures, human functions, and other resources) united by some form of regulated interaction to form an organized whole. A group of related processes.

References

- Statewide IT Information Security Glossary of Terms
- PTA & PIA User Guide for State Agencies
- PTA & PIA User Guide for NCDIT Employees