
Ohio Privacy Impact Statements and Assessments 2012

Privacy is about respecting the free choice of an individual to determine what information, in terms of physical characteristics, attitudes and behaviors, he or she will expose to others and when and to what degree information will be exposed. A privacy impact assessment (PIA) examines a business process or system of an agency with a focus on the perspective of the people whose information will be in the system. By conducting a PIA, an agency takes into consideration the consequences of their information collection and maintenance practices on both individuals and the agency.

To ensure privacy is considered, state agencies are required to create privacy impact statements in accordance with Section 125.18 of the Ohio Revised Code (ORC).¹ For the purposes of this guide, a Privacy Impact Assessment (PIA) is the same as a privacy impact statement. Section 1347.15 of the Ohio Revised Code² also requires state agencies to complete privacy impact assessment forms. Each state agency is required to have a Data Privacy Point of Contact (DPPOC) to assist the agency's program unit in completing a PIA.

Furthermore, performing a PIA upon the collection of new types of information or at the beginning of the development or acquisition of a new information system that maintains PII will help a state agency to determine most, if not all, of the necessary privacy and security controls. Specifically, a PIA:

- ensures handling of PII conforms to applicable legal, regulatory, and policy requirements regarding privacy;
- determines the risks and effects of collecting, maintaining and disseminating PII in both paper and electronic formats;
- examines and evaluates protections and alternative processes for handling information to mitigate potential privacy risks, such as the redaction of data prior to online publication as required by Section 149.45 of the Revised Code; and
- meets the specific requirements of ORC 125.18(C)(2) and ORC 1347.15(B)(8).

The most effective way to protect personally identifiable information (PII), in terms of both implementation and costs, is to incorporate privacy and security into the architecture and design of new or updated systems and business processes. Adding privacy and security after initial development can be more costly and problematic.

WHO AND WHAT IS ADDRESSED

As used in the PIA, "personally identifiable information" is information that can be used directly or in combination with other information to identify a particular individual. It includes:

- a name, identifying number, symbol, or other identifier assigned to a person,
- any information that describes anything about a person,
- any information that indicates actions done by or to a person,
- any information that indicates that a person possesses certain personal characteristics.

Examples of PII include:

- Publicly accessible data such as name, mailing address, zip code and telephone number.
- Data that may be particular to individuals but not necessarily sensitive, such as date of birth or internet protocol address.
- Data related to an individual's education, finances, health/medical, criminal or employment history.

¹ See <<http://codes.ohio.gov/orc/125.18>>

² See <<http://codes.ohio.gov/orc/1347.15>>

- Sensitive data elements that, when combined with any basic PII, can enable many services and benefits but also can cause serious harm in the wrong hands. Examples include: a social security number, federal tax identification number, financial account number, student identification number, health plan number, certificate/license number, vehicle identifier including license plate, biometric identifier (e.g., fingerprints), or any other unique identifying number or characteristic.

In this guide, Confidential Personal Information (CPI) is personal information that falls within the scope of section 1347.15 of the Revised Code and that an agency is prohibited from releasing under Ohio's public records law. State agencies should reference Rule 123-4-01 of the Ohio Administrative Code, "Accessing Confidential Personal Information,"³ for additional guidance on CPI.

A key difference between PII and CPI is that PII covers all types of information associated with a person, including information in public records and information that is exempt from disclosure under Ohio's public records law. Managing privacy entails more than non-disclosure of confidential information. Agencies have a responsibility to manage all aspects of privacy including data minimization, accuracy and data integrity, notice, choice and rights to review and correct. Regardless of whether PII is a public record or not, state agencies should address all forms of PII in PIAs because an additional level of care is necessary when handling all personal information.

This guide replaces Ohio IT Bulletin ITB-2008.02, "Privacy Impact Assessments," and all prior privacy impact assessments for existing systems (PIA-ES) forms.

Agencies are not required to do a wholesale replacement of completed PIAs for current business processes and systems with the new form. However, the agency should consider updating PIAs with the new form on a scheduled basis.

RECOMMENDED ACTIONS

As a first step in the PIA process, if there is uncertainty that a PIA must be completed, a program manager or system owner should complete a Privacy Threshold Analysis to determine whether a full PIA is required. A properly completed and approved Privacy Threshold Analysis provides documentation that a system owner assessed whether or not a full PIA is required. Agencies may complete a full PIA without completing the Privacy Threshold Analysis. A PIA is unnecessary for information systems that do not collect or maintain PII. A PIA is also unnecessary for state-controlled public Web sites where the user is given the option of contacting the site operator for the limited purpose of asking questions or providing comments. Attachment A contains a Privacy Threshold Analysis template. Attachment B provides a PIA template.

State agencies shall perform a Privacy Threshold Analysis or PIA when they collect new information, when agencies develop, buy, or contract out for new information technology systems to handle collections of PII, or when agencies conduct ad hoc queries of commercial databases containing PII. Even though in some instances PII exists only for a moment, a PIA shall still be performed. For example, an agency might be considering using a scanning device that temporarily captures images of people's bodies. In that instance a PIA should still be performed because PII is being collected even though the intention may be not to retain it beyond a moment. Examples of technology with privacy implications include systems utilizing radio frequency identification devices (RFID), biometric scans, data mining, and geospatial tracking.

A PIA shall address the following concerns:

- what information is collected by the information system;
- whether the information system contains PII as defined in this guide;
- why the information is collected by the state agency;

³ <http://codes.ohio.gov/oac/123-4>

- intended uses of the information;
- with whom the information will be shared, such as other agencies or contractors;
- what opportunities individuals have to decline to provide PII or to consent to particular uses of their information, and how this consent is granted;
- how the information will be secured;
- the retention schedule for maintaining PII;
- methods for disclosure and destruction of PII; and
- identification of a system with CPI under ORC 1347.15 and the status of compliance with that statute.

The treatment and use of PII in information systems under development may not be fully understood during the creation of the PIA. To compensate for this limitation, state agencies shall rely on documentation related to the system's development, including, as appropriate, a statement of need, functional requirements analysis, cost-benefit analysis, or an initial risk assessment. The PIA shall describe the impact the system will have on PII in the system, specifically identifying and evaluating potential threats to the extent these elements are known at the initial stages of development. Upon deployment of the system, the PIA shall be updated with elements not identified at the concept stage (e.g., retention or disposal of information), to reflect new information collection, or other choices made in designing the system or information collection. Agencies shall make documentation available upon request for audit in a timely manner.

The degree of specificity necessary for the PIA will vary according to two factors: the amount of personal information the proposed system will maintain, and the development stage of the information system itself. An information system that maintains significant amounts of personal information or that performs data-mining routines shall have a more detailed PIA.

AUTHORITY AND REFERENCE

ORC 125.18; ORC 149.011; ORC 149.434; ORC 1347; Ohio IT Standard ITS-SEC-01, "Data Encryption and Cryptography"

INQUIRIES

Direct inquiries about this guide to:

Chief Privacy Officer
Office of Information Security & Privacy
Office of Information Technology
30 East Broad Street, 40th Floor
Columbus, Ohio 43215
Telephone: 614-644-9391
E-mail: Chief.Privacy.Officer@oit.ohio.gov

This guidance and other Ohio privacy and IT security policies, standards and resources are found online at: <http://www.privacy.ohio.gov/Government.aspx>

(This page intentionally left blank).

Attachment A

Privacy Threshold Analysis (PTA)

Project or
System Name:

| | |
|--|--|
| | |
|--|--|

This form is used to determine whether a Privacy Impact Assessment is required.

Publication Date:

| | |
|--|--|
| | |
|--|--|

Contact Point

| | | |
|----------------------|--|--|
| Contact Person: | | |
| Agency and Division: | | |
| Contact Phone: | | |
| Contact E-mail: | | |

Data Privacy Point of Contact (DPPOC)

| | | |
|-------------------------------|--|--|
| Name of DPPOC: | | |
| Title of DPPOC: | | |
| Agency and Division of DPPOC: | | |

The purpose of a Privacy Impact Assessment is to determine the privacy implications of collecting Personally Identifiable Information (PII), including why PII is collected and how it will be used and secured. PII is defined as "personally identifiable information" and is information that can be used directly or in combination with other information to identify a particular individual. It includes:

- a name, identifying number, symbol, or other identifier assigned to a person,
- any information that describes anything about a person,
- any information that indicates actions done by or to a person,
- any information that indicates that a person possesses certain personal characteristics.

This document helps identify PII in a given information system.

The Ohio Office of Information Technology designed and tested this document in Microsoft Word 2007. Agencies should complete the shaded portions of this document and then submit a copy to your agency's Data Privacy Point of Contact.

Summary Information

| | |
|-----------------------------------|--|
| Date submitted for review: | |
| Name of Project: | |
| Name of Component: | |
| Name of Project Manager: | |
| E-mail for Project Manager: | |
| Phone number for Project Manager: | |

Specific Questions

1. Describe the project and its purpose:

Please provide a general description of the project and its purpose in a way a non-technical person could understand.

| |
|--|
| |
|--|

2. Status of Project:

This is a new development effort.

This is an existing project.

| | |
|-----------------------|--|
| Date first developed: | |
| Date last updated: | |

Please provide a general description of the update.

| |
|--|
| |
|--|

3. If this project is a technology/system, does it relate solely to infrastructure? [For example, is the system a Local Area Network (LAN) or Wide Area Network (WAN)]?

No. Please continue to Question 4.

Yes. Is there a log kept of communication traffic?

No. Please continue to Question 4.

Yes. What type of data is recorded in the log? (Please choose all that apply.)

Payload - Please describe the data that is logged.

Please list the data elements in the log.

4. Could the project relate in any way to an individual?

No.

Yes. Please provide a general description, below.

Please provide a general description of the way the project could relate to an individual.

5. Do you use or collect any of the following information:

- First and last name?
- Date of birth?
- E-mail address?
- Street address?
- Internet protocol (IP) address?
- Social Security Numbers (including truncated SSNs)?
- Federal Tax Identification Numbers?
- Driver's license numbers?
- A state identification card number issued under section 4507.50 of the Revised Code?
- Financial information, ranging from account numbers, credit card numbers and debit card numbers to credit history and credit scores?
- Student identification numbers?
- Health and medical information, ranging from medical account numbers and health plan numbers to diagnoses, health conditions and drug prescriptions?
- Certificate/license numbers?
- Employment information?
- Criminal information?
- Vehicle identifier including license plate?
- Biometric identifier (e.g., fingerprints)?
- Any other unique identifying number or characteristic that, when combined with any basic personally identifiable information, may cause serious harm in the wrong hands?

No.

Yes. Why does the program collect this information?

Please provide the reason for collecting this information and the legal authority to do so.

6. What information about individuals could be collected, generated or retained?

Please provide a specific description of information that might be collected, generated or retained such as names, addresses, e-mails, etc.

Privacy Threshold Review

Based on questions 1 – 6, does the project or system involve personally identifiable information and therefore warrant additional examination and documentation in the form of a Privacy Impact Assessment? [If you indicated that one or more of the examples from Question 5 are being collected by your agency, indicate “Yes” in the designation below.]

Designation:

No. This is NOT a Privacy Sensitive Project or System - the project or system does not contain Personally Identifiable Information.

Yes, this IS a Privacy Sensitive Project or System.

The following actions or designations apply (check all relevant boxes):

PTA sufficient at this time

A PIA is required

Additional Comments

(This page intentionally left blank).

Attachment B

Project or System Name: Privacy Impact Assessment for the

Publication Date:

Contact Point for Project or System

| | |
|----------------------|--|
| Contact Person: | |
| Agency and Division: | |
| Contact Phone: | |
| Contact E-mail | |

Data Privacy Point of Contact (DPPOC)

| | |
|-------------------------------|--|
| Name of DPPOC: | |
| Title of DPPOC: | |
| Agency and Division of DPPOC: | |

State of Ohio

The purpose of a Privacy Impact Assessment is to determine the privacy implications of collecting Personally Identifiable Information (PII), including why PII is collected and how it will be used and secured. PII is defined as "personally identifiable information" and is information that can be used directly or in combination with other information to identify a particular individual. It includes:

- a name, identifying number, symbol, or other identifier assigned to a person,
- any information that describes anything about a person,
- any information that indicates actions done by or to a person,
- any information that indicates that a person possesses certain personal characteristics.

This document helps identify PII in a given information system.

The Ohio Office of Information Technology designed and tested this document in Microsoft Word 2007. Agencies should complete the shaded portions of this document and then submit a copy to your agency's Data Privacy Point of Contact.

Abstract

The abstract should be no longer than five sentences and should address the following three items:

- The name of the component and system.
- A brief description of the system and its function.
- An explanation as to why the PIA is being conducted.

Overview

The overview is the most important section of the PIA. A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA. The overview should contain the following elements:

- The system name and the name of the agency who own(s) the system;
- The purpose of the program, system, or technology and how it relates to the agency's mission;
- A general description of the information in the system;
- A description of a typical transaction conducted on the system;
- Any information sharing conducted by the program or system;
- A general description of the modules and subsystems, where relevant, and their functions; and
- A citation to the legal authority to operate the program or system.

Section 1.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected as well as reasons for its collection as part of the program, system, rule, or technology being developed.

1.1 What information is collected, used, disseminated, or maintained in the system?

1.2 What are the sources of the information in the system?

1.3 Why is the information being collected, used, disseminated, or maintained? Is there a specific legal mandate or business purpose that requires the use of this information?

1.4 How is the information collected?

1.5 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

1.6 Conclusion: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

Section 2.0 Uses of the Information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

2.2 How will the information be checked for accuracy?

2.3 What types of tools are used to analyze data and what type of data may be produced?

2.4 If the system uses commercial or publicly available data please explain why and how it is used.

2.5 Conclusion: Describe any types of controls that may be in place to ensure that information is handled in accordance with the described uses in 2.1.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What information will be retained?

3.2 How long will information need to be retained?

3.3 Has the retention schedule been approved through the state records program?

3.4 Is the information deleted in a secure manner, i.e., in accordance with Ohio IT Policy ITP-E.1, "Disposal, Servicing and Transfer of IT Equipment," once the retention period is over?

3.5 Conclusion: Please discuss the privacy risks associated with the length of time data is retained and how those risks are mitigated.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the agency.

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

4.2 How is the information transmitted or disclosed?

4.3 Conclusion: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for external information sharing, including sharing with other state agencies in Ohio, agencies in other states, the Federal government, local governments, and private sector entities.

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

5.2 Is the sharing of personally identifiable information outside the agency compatible with the original collection? If so, is it addressed in a data-sharing agreement? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of the agency.

5.3 How is the information shared outside the agency and what security measures safeguard its transmission?

5.4 How does the agency verify that an external organization has adequate security controls in place to safeguard information? For example, is the external organization able to demonstrate compliance with SAS 70-II?

5.5 Conclusion: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

Section 6.0 Notice

The following questions are directed at notice to the individual who is the subject of information collected, the right to consent to uses of his or her information, and the right to decline to provide information.

6.1 Was notice provided to the individual prior to collection of information?

6.2 Do individuals have the opportunity and/or right to decline to provide information?

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

6.4 Conclusion: Describe how notice is provided to individuals, and how the privacy risks associated with individuals being unaware of the collection are mitigated.

Section 7.0 Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about him or her.

7.1 What are the procedures that allow individuals to gain access to their information?

7.2 What are the procedures for correcting inaccurate or erroneous information?

7.3 How are individuals notified of the procedures for correcting their information?

7.4 If no formal redress is provided, what alternatives are available to the individual?

7.5 Conclusion: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

Section 8.0 Security Implementation

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system and are they documented?

8.2 Will contractors have access to the system?

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

8.4 What auditing measures and technical safeguards are in place to prevent misuse of data?

8.5 Does the project employ technologies which may raise privacy concerns? If so please discuss their implementation.

8.6 Conclusion: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

Section 9.0 Protection of “Confidential Personal Information”

The following questions are directed at assisting agencies with compliance with section 1347.15 of the Ohio Revised Code.

9.1 Has the agency evaluated the personal information and the system it is in for application of ORC 1347.15?

a) Is the information the agency maintains “personal information” as defined by ORC 1347.01?

b) Is the information part of a “system” as defined by ORC 1347.01?

c) Is the information “maintained” in the system as defined by ORC 1347.01?

d) Is the information not a public record for purposes of Section 149.43 of the Revised Code?

If the answer is “yes” to all 4 questions, then the system contains CPI. If the answer is “no” to any of the 4 questions, the system does not contain CPI and you have completed Section 9.

9.2 Has the agency documented and labeled the confidential personal information in this system? If so, please provide the name and date of the documentation and a point of contact (name, e-mail, phone).

9.3 Does the agency maintain a set of criteria for determining which employees of the state agency may access, and which supervisory employees of the state agency may authorize those employees to access, confidential personal information in this information system? Please provide the name and date of the documentation with the criteria and a point of contact (name, e-mail, phone).

9.4 Is there a written policy that specifically addresses a list of the valid reasons, directly related to the state agency's exercise of its powers or duties, for which only employees of the state agency may access the confidential personal information found in this information system?

9.5 Has the agency cataloged the federal or state statutes or administrative rules that make the confidential personal information confidential? If so, please provide the name and date of the catalogue and a point of contact (name, e-mail, phone).

9.6 Does this information system have a mechanism for recording specific access by employees of the state agency to confidential personal information?

This procedure should include two exceptions for manual logging:

- a) where access both
 - (i) results from research, routine office procedures or incidental contact and
 - (ii) results from conduct not specifically directed toward a specifically named individual or a group of specifically named individuals; and

- b) where access occurs as a result of a request by the individual for CPI about that individual.

9.7 Is the CPI in this information system available for inspection by the subjects of the information?

9.8 Is there a procedure for notifying each person whose CPI in the information system has been accessed for an invalid reason by employees of the state agency?

9.9 Is access to this information system controlled by a password or other authentication measure?

9.10 Does the agency have administrative rules published that are consistent with Ohio Revised Code 1347.15?

9.11 Has the agency published its policies on its web site and posted posters regarding its policies?

9.12 Have employees of the state agency with access to CPI in this information system been trained on the applicable statutes, rules and policies governing their access to that CPI?

9.13 Have employees of the state agency received a copy of policies and procedures related to CPI as required by ORC 1347.15? Have they acknowledged receipt of such policies?

9.14 Conduct a periodic examination of the business need and legal basis for collecting CPI so that opportunities to eliminate CPI are identified. Next Date of Data Minimization Review:

9.15 Conclusion: Given the amount of CPI collected, discuss the privacy risks identified and how they were mitigated above and beyond what is required for PII.