2012 Data Privacy Point of Contact Training Agenda

Riffe Center, Room 1948
April 26, 2012 - 8:30 a.m. to 12:00 p.m.

I. Welcome and Review of the Day's Agenda

8:30 a.m. to 8:40 a.m.

II. Privacy Concepts

8:40 a.m. to 9:30 a.m.
Introduction of a number of privacy concepts including:

- what the potential harms are to individuals;
- how to make the case for privacy within your agency;
- defining privacy and addressing common misconceptions; and
- a framework for applying privacy to an agency's business practices.

III. Managing Privacy Programs

9:30 a.m. to 10:15 a.m.
This session will cover:

- a review of the State Privacy program, including resources that the Office of Information Security & Privacy have available for state agencies to use;
- open discussions on the role that Data Privacy Points of Contact can play within an agency, and how specific privacy-related processes are handled by certain agencies; and
- strategies on implementing a privacy program.

IV. Break

10:15 a.m. to 10:30 a.m.

V. Good Privacy Practices: Beyond Compliance

10:30 a.m. to 11:30 a.m.
This session will cover:

- a review of statewide requirements such as those found in Ohio Revised Code 1347 and state information technology policy;
- Practices such as notice, use and secondary use, consent, use of contractors with personal information, and other privacy-related concerns; and
- a discussion of how security can be leveraged to protect privacy.

VI. Privacy Trends and Challenges

11:30 a.m. to 12:00 p.m.
The final session will begin with an update on privacy trends. Open discussion will focus on current and upcoming areas of privacy concern, including technological changes such as mobile applications and devices, social media, and geo-tracking, and legal and societal trends such as court cases, federal legislation and public attitudes.

VII. Wrap-up

PRIVACY: RESPECT +PROTECT

2012 Ohio Privacy Seminar

OhioDAS Office of Information Technology | Office of Information Security and Privacy Service · Support · Solutions

---

PRIVACY: RESPECT +PROTECT

OhioDAS Office of Information Technology | Office of Information Security and Privacy Service · Support · Solutions

Roadmap for Today/Other Sessions

- Logistics
- Goals for today
- Expectations for other sessions

PRIVACY: RESPECT +PROTECT

Agenda / Purpose

- Daren Arnold, Chief Privacy Officer, Department of Administrative Services
- Privacy Concepts
- Privacy Program Management
- Privacy Practices and Compliance
- Privacy Trends and Challenges

OhioDAS Office of Information Technology | Office of Information Security and Privacy Service · Support · Solutions

PRIVACY: RESPECT +PROTECT

Privacy Concepts

OhioDAS Office of Information Technology | Office of Information Security and Privacy Service · Support · Solutions

2012

Agenda / Purpose

Privacy Defined

Privacy Harms

Fair Information Practice Principles

The Case for Privacy

Privacy Misconceptions

- Daren Arnold, Chief Privacy Officer, Department of Administrative Services
- Privacy Concepts
  - Privacy Defined
  - Privacy Harms
  - Fair Information Practice Principles
  - The Case for Privacy
  - Privacy Misconceptions

Agenda / Purpose

What is Privacy?

- What is Privacy?

The Necessity of Privacy

- The state collects a vast amount of PI:
  - Birth records
  - Death records
  - Driver's license data
  - Education data
  - Tax data
  - Law Enforcement:
    - Criminal
    - Victim
    - Accused
  - Health:
    - Health conditions/impairments
    - Medicaid
  - Financial data
  - Professional licenses
  - Familial data:
    - Marriage
    - Divorce
    - Child support
    - Foster
    - Seniors
  - Employee data

What is privacy?

4 Key Concepts

- Privacy Defined
- Privacy Harms
- Information Lifecycle
- Fair Information Practice Principles

PRIVACY: RESPECT +PROTECT

OhioDAS Office of Information Technology | Office of Information Security and Privacy

What is privacy?

- Seems like an intuitive definition:
  - A "zone" around you…
  - …Your house…
  - ……your physical state…
  - ……your tax returns…
  - ……personal e-mails…
  - …….your Facebook page…
  - ……who did you vote for?

PRIVACY: RESPECT +PROTECT

OhioDAS Office of Information Technology | Office of Information Security and Privacy

What is privacy?

Privacy defined:

- "Privacy" is the recognition that a free and democratic society requires:
  - a) respect for the autonomy of individuals and
  - b) limits on the power of both state and private organizations to intrude on the free choice of the individual
    - specifically the circumstances and degree to which the individual will expose his physical characteristics, attitude and behavior to others.

Agenda / Purpose

Privacy Defined

Privacy Harms

Fair Information Practice Principles

The Case for Privacy

Privacy Misconceptions

- How do you harm someone's privacy?

Privacy Harms

- Violating a person's privacy can:
  - Limit a person's freedom
    - Decision to disclose or not
    - Speech, association, religion, travel, general life choices
  - Lead to fraud (e.g., identity theft)
    - Financial, medical, criminal
  - Cause relational harm and societal friction for individual
    - Tension, rejection, assumptions, prejudices
    - Family, workplace, friends, community
  - Pose a risk to physical safety
    - Domestic abuse, stalking, robbery
    - Erroneous medical services
  - Create a burden and cost to correct
  - Create a power imbalance

Agenda / Purpose

Privacy Defined

Privacy Harms

Fair Information Practice Principles

The Case for Privacy

Privacy Misconceptions

- FIPPs: A Framework for Understanding Privacy

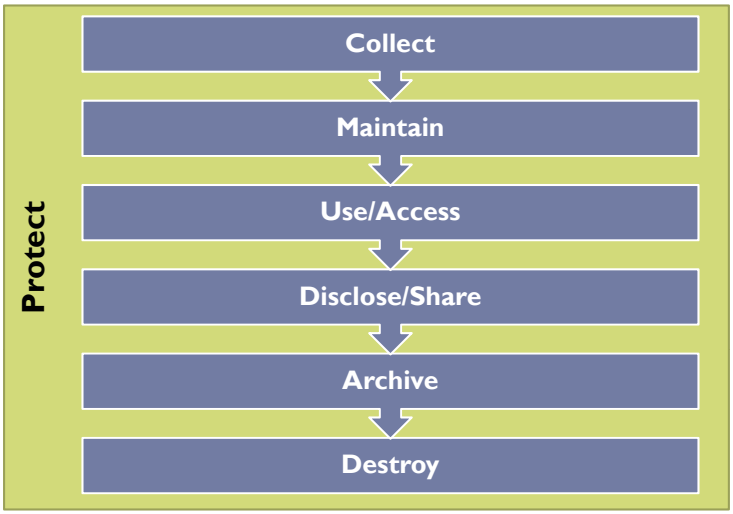
Fair Information Practice Principles

- Nondisclosure
  - Matter of degrees, more than secrecy
- Use and Purpose
  - Use PI only for stated purposed, limit uses for other purposes
- Transparency
  - Upfront about information practices & right to review
    - What information is collected, how it's collected, and how it's used
- Participation
  - "Respecting autonomy" means meaningful choice
- Integrity, Relevance, Accuracy, Completeness
- Security
- Data Minimization
- Accountability and Auditing

Fair Information Practice Principles

- **Code of Fair Information Practice Principles**
  - Framework for leveraging privacy into your business processes, information systems, and future plans.
  - Consider applying the FIPPs wherever personal information is used within your organization.
  - Think about it throughout today's sessions!

Information Lifecycle



Harms, FIPPs, Lifecycle

How they relate

- Harms can occur anywhere along lifecycle
- Harms result from intentional & unintentional conduct
- Harms can result from failure to follow FIPPs
- Effective use of FIPPs can mitigate some harms
  - Aggressive use of other FIPPs when privacy risks are high
- Continuum for harm, risk and FIPPs mitigation

Agenda / Purpose
Privacy Defined
Privacy Harms
Fair Information Practice Principles
The Case for Privacy
Privacy Misconceptions

The Case for Privacy?

- Mark Zuckerberg: "People have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people. That social norm is just something that has evolved over time."

The Case for Privacy

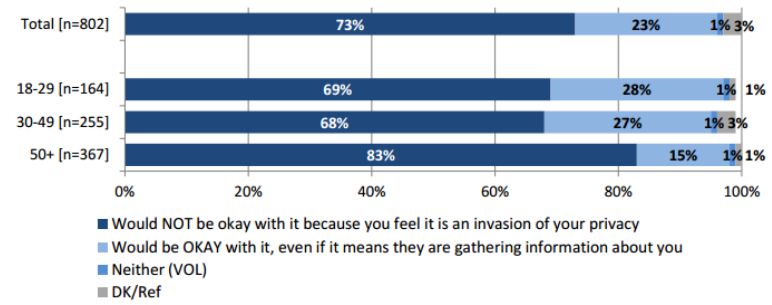
- **Social Networking**
- "Facebook's user base is so large that, were it a country, it would be the third most populous nation in the world."
  - *Survey from the Health Care Compliance Association & the Society of Corporate Compliance and Ethics*
- In 2011, 63% of people in a Pew survey deleted people from their "friends" lists.
- A majority of social network site users – 58% – restrict access to their profiles.
- 11% of SNS users have posted content they regret.
- Zuckerberg's profile is restricted on Facebook

The Case for Privacy

Three-quarters of search users say collecting user information to personalize search results is not okay

If a search engine kept track of what you search for, and then used that information to personalize your future search results, how would you feel about that?

Based on search users [n=802]



Source: The Pew Research Center's Internet & American Life Project Winter 2012 Tracking Survey, January 20-February 19, 2012. N=2,253 adults, age 18 and older, including 901 cell phone interviews. Interviews conducted in English and Spanish.

The Case for Privacy

Risk for Agencies

- Breaches
- Missteps
- "Secrecy"
- Legal Violations

Consequences

- Loss of trust
- Criminal or civil liability (agency and employees)
- Individuals' jobs
- Reputation
- Program risks
- Added accountability requirements

The Case for Privacy

Conclusions

- The public is becoming increasingly sensitive to the harms caused by privacy failures.
- The public has not abandoned expectations of privacy.
- Promoting privacy is responding to a customer demand.
- Privacy builds trust.

Agenda / Purpose

Privacy Defined

Privacy Harms

Fair Information Practice Principles

The Case for Privacy

Privacy Misconceptions

- Privacy Misconceptions

Privacy Misconceptions

Misconception	Concept
Privacy means "not disclosing secret info."	**Privacy is about respecting the *choice* of a person regarding collection, disclosure and use.** Examples: Collection – secret surveillance in a locker room Disclosure – a distant work acquaintance asks "how are you today?" You start to say "fine" but a friend explains that you might be coming down with the flu and that you are struggling with depression. Use – home phone number in public directory and on Do-Not-Call list.

Privacy Misconceptions

Misconception	Concept
2 categories: secret or public knowledge	**There are levels of disclosure.** Examples, conversations in crowded restaurant 2-person table vs. group table vs. loud guy at bar vs. band with audio system.
If PI is public in one context, it should be treated as public all other contexts.	**Context matters.** Home address (property owner vs. patient) **Capabilities differ.** Single record look-ups available for review in an office are different than a database available for download by anyone online.

Privacy Misconceptions

Misconception	Concept
"Privacy is dead."	**Everyone exercises privacy choices every day.**
"Free" websites and apps	**Personal information has real value. Exchanges of PI come with explicit and implicit agreement.** Example, what is Facebook's value if it had no personal information?
Because technology enables us to do X, we should do X.	**Technology changes continually and has both potential positive and negative impacts on individuals. Evaluate both. Are there ways to use while minimizing privacy risks?**

Privacy Misconceptions

Misconception	Concept
Subjective reaction, "I don't care if someone knows everything about me."	**People face different circumstances where privacy (improper use or disclosure) can mean life or death or be costly in terms of time, money, relationships, reputation (right or wrong), employment, etc.** Examples, battered women, informants, mental health patients, political dissidents, vulnerable (kids, elderly, learning disabled) etc.
Electronic info is easy to handle, carry, copy, etc., (consequence of carelessness).	**Personal info in electronic format is like a hazardous material.** It can be very useful if handled with care. It can be very harmful if mishandled, having a wide impact.

Privacy Misconceptions

Misconception	Concept
What do I need to do to comply with privacy laws?	**Privacy laws are just one part of privacy.** Also **consider citizen expectations and trust**, standard of due care and the right-thing-to-do, while avoiding hyper-reaction.

Privacy vs. IT vs. Info Security

Privacy: Related but Different Than IT and Info Security

- Covers all personal information regardless of format – paper, electronic, person-to-person
- Concerned with business processes, legal requirements, customer expectations
- Requires security but is more than that
- IT delivers data and tools in a manner the business units need
- Information Security is about:
  - The *means* of protecting *all types* of data and *systems*
  - *Manages all types of risk to entity*

Why is privacy important to your agency?

Key questions to think about:

- Who gets to see this information?
- Where is it kept?
- How is this personal information (PI) protected?
- How is the information used, shared and re-used?

PRIVACY: RESPECT +PROTECT

OhioDAS Office of Information Technology | Office of Information Security and Privacy

Why is privacy important to your agency?

Key questions to think about:

- When is the risk to customer / public considered?
- Who is responsible for representing John and Jill Public?
- How can multiple goals be reconciled?
  - Not a zero-sum game
  - Multiple stakeholders
  - Benefits of technology and innovation AND privacy

PRIVACY: RESPECT +PROTECT

OhioDAS Office of Information Technology | Office of Information Security and Privacy

Why is privacy important to your agency?

Rest of the morning:

- Your role as data privacy coordinator or other privacy influencer
- Privacy standards – legal compliance and more
- Privacy trends and developing issues

Questions?

PRIVACY: RESPECT +PROTECT

Privacy Program Management

OhioDAS Office of Information Technology | Office of Information Security and Privacy Service · Support · Solutions

2012

PRIVACY: RESPECT +PROTECT

Agenda / Purpose

State of Ohio Privacy Program

Role of the DPPOC

Panel Discussion: Agency Privacy Programs

Key DPPOC Tasks

- Privacy Program Management
  - State of Ohio Privacy Program
  - Role of the DPPOC
  - Panel Discussion: Agency Privacy Programs
  - Key DPPOC Tasks

OhioDAS Office of Information Technology | Office of Information Security and Privacy

The Necessity of Managing Privacy

- In the context of Ohio government agencies, privacy is about addressing the practices, issues and harms relating to PI in a manner consistent with:
  - the public's expectations,
  - Ohio law,
  - Federal law, and
  - standards of care in light of the particular risk to different types of PI.

The Necessity of Privacy

- Without intentional consideration of privacy, agencies will likely encounter potentially high-profile problems, including:
  - employees using personal information for their own profit;
  - databases being hacked;
  - laptops, CDs or thumb drives lost with unencrypted sensitive personal data;
  - employees snooping into files of friends, family members and famous people; (continued…)

Ohio's open record laws linked to identity theft

10:52 PM, May. 8, 2010 | 6 Comments

Written by Eileen Kelley

FILED UNDER

News
Local News

Ohio's open public record laws are being blamed for giving a new identity to an Oregon man who was arrested recently for allegedly stealing the identity of a Springfield Township boy who was kidnapped and killed nearly 28 years ago.

Twitter
Facebook
Share
Email

The Necessity of Managing Privacy

Fired Cincinnati police officer jailed for snooping on woman

Thursday, May 5, 2011 04:00 PM

Associated Press

CINCINNATI -- A fired Cincinnati police officer has been sentenced to seven months behind bars for using his police cruiser computer to look up personal information that authorities say he used to harass a woman.

- government officials illegally monitoring the legal activity of citizens;
- collecting sensitive Personally Identifiable Information (PII) without justification; and
- carelessly disclosing PII as part of a business process to individuals or even on the Web.

Agenda / Purpose

State of Ohio Privacy Program

Role of the DPPOC

Panel Discussion: Agency Privacy Programs

Key DPPOC Tasks

- State of Ohio Privacy Program

Privacy Program: CPO Mission

- Mission of the Enterprise Privacy Program…
  To lead and advance the State of Ohio in safeguarding the people's privacy.
- History
  - 2007: 1st CPO
  - 2008: Codified
  - 2009: Added duties. DPPOCs required
  - 2010: Office of Information Security & Privacy established
- Advises agencies, DAS senior management and decision-makers in the executive and legislative branch pertaining to privacy matters.
- The Ohio Privacy Advisory Board works to identify and address common privacy-related concerns across state agencies.

Privacy Program

- Raises agencies' awareness of the need to consider privacy matters in business processes and use of information technology.
- Principally:
  - provides advice and privacy management resources to the data privacy point of contact within each agency;
  - provides assistance on incident response efforts; and
  - upon request, provides recommendations on policy and legislative matters relating to privacy and personal information.

Privacy Program

- Promotes agencies' communication:
  - to the public regarding the rights that individuals have pertaining to personal information and privacy;
  - of the responsibilities that managers have to limit, protect and ensure the proper use of personal information; and
  - of agency policies applicable to employees about their duty to protect privacy.

Privacy Program: 2012 Key Activities

- Conduct privacy education and training programs.
- Improve the use of the privacy impact assessments as a discipline within state agencies.
- Advocate the consideration of privacy when new state initiatives are created.
- Strengthen privacy practices for current, key business processes (hard copy files, web privacy statements).
- Continue to assist agencies with the implementation of ORC 1347.15.

Agenda / Purpose

State of Ohio Privacy Program

Role of the DPPOC

Panel Discussion: Agency Privacy Programs

Key DPPOC Tasks

- Role of the DPPOC

Role of the DPPOC

Three aspects to the DPPOC role:

- Coordinator: Required by statute to work to ensure CPI is properly protected and that the agency complies with ORC 1347.15
- Promoter: Also useful in terms of building trust with customers and enhancing agency reputation
- Responder: A troubleshooter for privacy complaints or incidents

Role of the DPPOC

What is the role of the DPPOC?

- Advocates for the public's privacy within the agency
- Advises or evaluates changes to a business process for privacy implications
- Handles requests for access to or correction of PI
- Liaison to the State Chief Privacy Officer
- Works with others in the agency to conduct PIAs
- Raises awareness of compliance

Role of the DPPOC

Who should serve as the DPPOC:

- Could be legal, IT or with a business unit
- Must understand what the agency collects, especially the legal basis (ORC 1347.15)
- Requires familiarity with the agency's legal privacy requirements
- Requires enough familiarity with technology
- Can advocate appropriate solutions

Role of the DPPOC

Help for DPPOCs:

- Ongoing training sessions
- OISP staff
- Resources online
- Ohio Privacy Advisory Board form for legislative questions

Agenda / Purpose

State of Ohio Privacy Program

Role of the DPPOC

Panel Discussion: Agency Privacy Programs

Key DPPOC Tasks

- Panel Discussion: Agency Privacy Programs

Agenda / Purpose

State of Ohio Privacy Program

Role of the DPPOC

Panel Discussion: Agency Privacy Programs

Key DPPOC Tasks

- Key DPPOC Tasks

Privacy Practices

A few important Privacy Practices that we'll cover in this section:

- Developing privacy policies and procedures
- Conducting Privacy Impact Assessments

Privacy Policies and Procedures

Overview of ORC 1347.15 requirements:

- Identify "covered systems" with confidential personal information maintained by the agency
- Develop rule and policy guidance for employees
- Complete of Privacy Impact Assessments
- Implementing privacy & security solutions
  - Technologies and business processes
  - Authentication/passwords logging access management
- Employee education of rules and policies
- Posting of policies on Internet
- Demonstrating compliance

Privacy Policies and Procedures

ORC 1347.15 policies and procedures:

- Template Policy on Protecting Privacy
  - Covers Personally Identifiable Information, Sensitive Personally Identifiable Information, Confidential Personal Information
- Procedures on:
  - Accessing and Logging CPI
  - Incident Response for Invalid Access of Confidential or Sensitive PII
  - Accessing CPI on Paper
  - Requests for PI
  - Accessing Sensitive Data
- Please visit http://www.privacy.ohio.gov/Government.aspx to download the templates

Privacy Policies and Procedures

Web site privacy statements:

- Required by State of Ohio IT Policy ITP-F.4, "Executive Branch Cabinet Agency Web Site Standardization"
- ORC 1347.08 also requires state agencies to notify individuals about the existence and types of uses made of personal information
- ALL agency websites should have a privacy policy

Privacy Policies and Procedures

Web site privacy statement should include the following elements:

- Type of information being collected
- Methods for collecting personal information
- Use of collected personal information
- CPI policies
- Inspection and dispute of PI
- Contact information
- Updates to the privacy notice
- Applicable laws and regulations
- Placement and labeling of the privacy notice
- Example: http://ohio.gov/policies/

Privacy Impact Assessments

- PIAs
- Required by ORC 125.18(C)(2)
- Data Privacy Points of Contact (DPPOCs) are required to complete PIAs by ORC 1347.15.
- The Ohio Privacy Impact Statements and Assessment 2012 (see http://privacy.ohio.gov/government)

PIA Process: What is a PIA?

Privacy Impact Assessments

- Identifies risks to individuals (not just business risks and goals).
- Evaluates information systems and business processes for privacy issues.
- Ensures agency handling of PI conforms with regulations.
- Evaluates alternate processes for handling information to mitigate risks (e.g., redaction).

PIA Process: What is a PIA?

- Help determine overhead of collecting, maintaining and sharing PI.
- PIAs are commonplace at the federal level, some states and companies.
- Informs selection of security controls.

PIA Process: What is a PTA?

Privacy Threshold Analysis (PTA):

- Screening process with 6 questions to determine if a system contains "personally identifiable information."
- Helps determine if a full PIA is required and documents that you made that assessment.
- If PII: complete the second part, the PIA.

PIA Process: PIA Components

Overview: summary description of the system	What information is collected and is it PII?
Why collected	Uses of the information
Notice of collection	Opportunities to decline to provide PII, consent to use, how consent is granted
Internal sharing/external sharing and disclosure	Security implementation (high-level)
Retention schedule	Methods of disclosure/destruction of PII

PIA Process: Benefits of a PIA

- The most effective way to protect information and systems is to work privacy/security into the architecture early on.
- Informs design of proposed systems.
- Compliance: meet ORC 125.18 and 1347.15 requirements.
- Documented that you assessed for privacy risks.
- Create privacy awareness, e.g., federal practice of publishing PIAs online.

PIA Process: When to Complete?

Think of major information lifecycle events:

- Collect new type of information
- Develop or procure an IT system
- Convert paper-based records to electronic
- Significant updates or merges to the system
- Increased access or new uses

Also conduct a PIA whenever you:

- De-anonymize or compile data
- Conduct ad hoc queries of commercial databases containing PII
- Temporary collections of PII (e.g., scans of a person's body)

PIA Process: When to Complete?

No PIA necessary when:

- No PII,
- System already assessed by an evaluation similar to PIA,
- State Web sites where user is given option of contacting site operator to ask questions or provide comments,
- Privacy issues are unchanged, i.e., no need for annual maintenance.

PIA Process: Best Practices

Leverage the following resources, if available:

- Project charter for the system
- Architectural specifications of the initiative
- Threat or risk assessments
- Business process analyses

Determine who is needed to provide input for different parts of the PIA and involve them: e.g., legal, business process owners, IT

Agenda / Purpose

State of Ohio Privacy Program

Role of the DPPOC

Key DPPOC Tasks

- In Conclusion

Role of the DPPOC

Three aspects to the DPPOC role:

- Coordinator: Required by statute to work to ensure CPI is properly protected and that the agency complies with ORC 1347.15
- Promoter: Also useful in terms of building trust with customers and enhancing agency reputation
- Responder: A troubleshooter for privacy complaints or incidents

Role of the DPPOC

What is the role of the DPPOC?

- Advocates for the public's privacy within the agency
- Evaluates privacy implications of changes to a business process
- Handles request for access to or correction of PI
- Liaison to the Chief Privacy Officer
- Conducts PIAs
- Awareness of compliance

Questions?

PRIVACY: RESPECT +PROTECT

Privacy Practices and Compliance

OhioDAS Office of Information Technology | Office of Information Security and Privacy Service · Support · Solutions

2012

Agenda / Purpose

Good Privacy Practices

Panel Discussion: Privacy and Legal Considerations

Ohio Privacy Laws

Federal Privacy Laws

- Privacy Practices and Compliance
  - Good privacy practices
  - Panel Discussion: Privacy and Legal Considerations
  - A review of Ohio privacy laws of concern to state agencies
  - A brief review of federal privacy laws

Agenda / Purpose

Good Privacy Practices

Panel Discussion: Privacy and Legal Considerations

Ohio Privacy Laws

Federal Privacy Laws

- Good Privacy Practices

Fair Information Practice Principles

- **Code of Fair Information Practice Principles (FIPPs)**
  - Eight privacy principles to follow when collecting, using or disclosing personal information:
    - Transparency
    - Individual participation
    - Purpose specification
    - Data minimization
    - Use limitation
    - Data quality and integrity
    - Security
    - Accountability and auditing
  - Basis for federal and state privacy laws
  - A few fundamentals you will always want to follow regardless of laws

A Few Fundamentals: Notice

Notice: Communicates an organization's privacy policies and procedures. The policies and procedures should identify the purpose for which personal information is collected, used, retained, and disclosed.

Characteristics of effective notice:

- Privacy policies are communicated to users
- Provided initially and in some cases periodically
- Clear and conspicuous
- Accurate and complete
- Readable and in plain language

Benefit: Transparency promotes trust. Secrecy promotes distrust.

FIPP: Transparency, Purpose Specification

PRIVACY: RESPECT +PROTECT

OhioDAS Office of Information Technology | Office of Information Security and Privacy

A Few Fundamentals: Consent

Consent: Any freely-given, specific, and informed indication that a person agrees to the processing of his or her personal data by an organization.

Typically provided through either:

- Opt-out – A method in which personal information will be used **unless** a person indicates it should be otherwise
- Opt-in – A method in which personal information will be used only **if** a person indicates it should be so

Benefit: Freedom – users make the choice as to whether their PI is used as described.

Caveat: Legal mandates – requirements to collect, disclose, etc. - may eliminate choice.

FIPP: Participation

PRIVACY: RESPECT +PROTECT

OhioDAS Office of Information Technology | Office of Information Security and Privacy

A Few Fundamentals: Use

Use and secondary use (critical to meeting ORC 1347.15 compliance!):

Once the agency has the PI:

- Use of personal information should be limited to an ***identified purpose*** (i.e., as stated in notice), subject to the ***consent*** of a person
- Use should ***strictly*** be for a defined purpose (e.g., identified in statute or administrative rule)
- Retention should only be for as long as the information is reasonably needed
- Data that is not retained should be securely disposed, returned, or destroyed

Benefit: Minimize the potential for misuse of PI or other privacy harms. Implied promise – broken if use in another way. Context of collection for first use may not translate accurately for second use.

FIPP: Use Limitation

Devaluing Personal Data

Data minimization – how can we decrease the risk of PI misuse and yet still maintain it?

- Can we limit the ***amount*** of identifiable data maintained as well as the ***time period*** for which it is retained to promote privacy?
- Data Minimization involves practices such as:
  - Evaluate need for data, eliminating data altogether, when possible.
  - De-identification, pseudonymity, and anonymity.
  - Reduce access – limit who has access, limit what is displayed.

Security

Encryption:

- Ohio IT Policy ITB-2007.02, "Data Encryption and Securing Sensitive Data" provides guidance on using encryption:
  - Use state-approved strong encryption
  - Secure portable devices and media
  - Secure sensitive data in transmission and, where feasible, data at rest
- Encryption can save you from having to notify due to a breach!
- Keep keys and passwords separate from encrypted data/devices
- Be diligent about incorporating use of encryption in contracts
- How encryption is implemented can carry significant trade-offs:
  - Field encryption permits granularity at the expense of performance.
  - File encryption avoids having to change the application.
  - Disk encryption is least granular approach but generally not difficult to implement.

Security

David Shaw
State Chief Information Security Officer

Agenda / Purpose

Good Privacy Practices

Panel Discussion: Privacy and Legal Considerations

Ohio Privacy Laws

Federal Privacy Laws

- Panel Discussion:
  Privacy and Legal Considerations

PRIVACY: RESPECT +PROTECT

Agenda / Purpose

Good Privacy Practices

Ohio Privacy Laws

Federal Privacy Laws

Ohio Privacy Laws

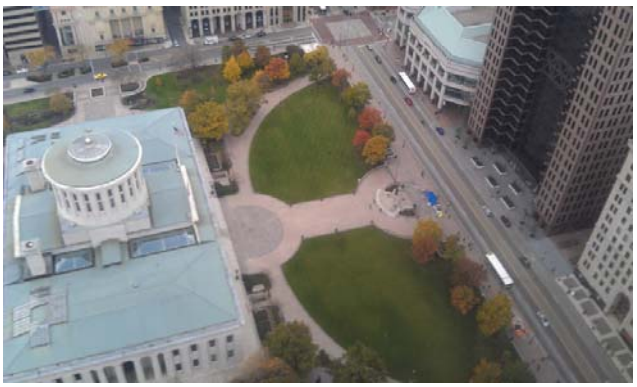


Photo credit: Jason Mather

OhioDAS Office of Information Technology | Office of Information Security and Privacy

PRIVACY: RESPECT +PROTECT

OhioDAS Office of Information Technology | Office of Information Security and Privacy

Ohio Privacy Laws

Two ways to think about state privacy regulations:

- **General requirements** to meet, and
- **Specific requirements** for certain agencies:
  - A law that requires an ***agency*** to keep a certain type of information confidential
  - A law that requires a ***certain type of information*** that an agency maintains to also be kept confidential

PRIVACY: RESPECT +PROTECT

OhioDAS Office of Information Technology | Office of Information Security and Privacy

Ohio Privacy Laws: Scope

ORC 1347 – Personal Information Systems

- Establishes the requirements for state agencies maintaining "personal information systems."
- Major Definitions – 1347.01
  - **Personal information** is defined as any information that describes anything about a person or indicated action done by or to a person, and is retrieved from a system by name or personal identifier.
  - A **system** means a collection or group of related records that are kept in an organized manner and that are maintained by a state or local agency and from which PI is retrieved by name/identifier.
  - Applies to both electronic and paper records.
- Specific exemptions for certain government entities – 1347.04
  - Includes criminal courts; prosecutors; any state or local agency or part of any state or local agency that is a correction, probation, pardon, or parole authority; others

PRIVACY: RESPECT +PROTECT

OhioDAS Office of Information Technology | Office of Information Security and Privacy

Ohio Privacy Laws: General Requirements

General requirements to meet:

- Affirmative duties placed on state and local agencies that maintain personal information systems (1347.05), for example:
  - Inform people whether they are required to submit information
  - Maintain PI with accuracy, relevance, timeliness, and completeness
  - Take reasonable precautions to protect PI
  - Appoint an individual responsible for the system
- Explicit rights of persons who are subject of personal information (1347.08), for example:
  - Inspect own PI
  - Learn how PI is used
- Provide means by which a person can dispute personal information (1347.09) or to challenge wrongful disclosure of personal information (1347.10)
- Public records law (149.43) and exemptions

Ohio Privacy Laws: General Concerns

Certain things state agencies **can** and **cannot do**:

- Strict use of personal information (1347.05,1347.07, 1347.071, 1347.15)
- Access rules for confidential personal information (1347.15)
- Disclosure of a security breach of computerized personal information (1347.12)

Ohio Privacy Laws: General Concerns

Use of Personal Information

- A state or local agency **shall only use** the personal information in a personal information system in a manner that is consistent with the purposes of the system. (ORC 1347.07)
- No placement or use of personal information in an interconnected or combined system (1347.071), **unless:**
  - the system will contribute to the efficiency of the involved agencies in implementing authorized programs;
  - the personal information is necessary and relevant to the performance of a lawful function; and
  - the agency must inform the citizen about the system and the other agencies or organizations with access.

Ohio Privacy Laws: General Concerns

ORC 1347.15 - Access rules for confidential personal information

- Access rules for confidential personal information
- Covers "systems" from which CPI is retrieved by name or personal identifier
- Strict "need to know" access requirements
- Procedural safeguards for accessing and using CPI
  - Logging access to CPI
- Each agency is required to train their employees on the statute
- Enforcement and penalties for non-compliance
- Standards for liability under this section: criminal, civil liability, and employment consequences

Ohio Privacy Laws: General Concerns

ORC 1347.15 - Access rules for confidential personal information

- Strict requirements for procedures to log employee access to personal information 1347.15 (b)
- Logging how-to:
  - 1347.15 sets strict logging requirements upon agencies maintaining and accessing personal information.
  - Old systems – manual logging with limited exceptions
  - New or updated systems – automatic logging, no exceptions
  - The Logging Methods Recommendation provides a detailed description on how to properly log employee access to confidential personal information.

PRIVACY: RESPECT +PROTECT

OhioDAS Office of Information Technology | Office of Information Security and Privacy

Ohio Privacy Laws: General Concerns

Ohio Revised Code 1347.12 – Security Breach Notification

- A state agency or political subdivision **must disclose a breach** of personal information
- Definitions are critical:
  - "Personal information" – Here limited to *computerized* PI covering:
    - SSN, driver's license number, state ID card, financial/credit card/debit card account number with access code
    - Not encrypted; not redacted
  - "Breach of the security of the system" defined in statute
    - Use "incident" until a determination has been made

PRIVACY: RESPECT +PROTECT

OhioDAS Office of Information Technology | Office of Information Security and Privacy

Ohio Privacy Laws: General Concerns

Ohio Revised Code 1347.12 – Security Breach Notification

- A state agency or political subdivision **must disclose a breach** of personal information
  - To whom: Any resident of this state whose personal information was, or reasonably is believed to have been, **accessed and acquired by an unauthorized person** if the access and acquisition by the unauthorized person **causes or reasonably is believed will cause a material risk of identity theft or other fraud to the resident**
  - When: In the most expedient time possible but **not later than forty-five days** following its discovery or notification of the breach in the security of the system (law enforcement investigatory delay)
  - How: written, electronic, telephone, or substitute notice

PRIVACY: RESPECT +PROTECT

OhioDAS Office of Information Technology | Office of Information Security and Privacy

Ohio Privacy Laws: General Concerns

Ohio Revised Code 1347.99 – Consequences for violating certain sections of Chapter 1347

- If any public official or person who maintains a personal information system violates 1347.05, 1347.071, 1347.08, or 1347.09, they may be guilty of a minor misdemeanor.

Any employee who violates a confidentiality statute or the agency's ORC 1347.15 rule is subject to:

- criminal charges,
- civil liability arising out of the employee's actions,
- employment termination, and
- a lifelong prohibition against working for the State of Ohio.

PRIVACY: RESPECT +PROTECT

OhioDAS Office of Information Technology | Office of Information Security and Privacy

Ohio Privacy Laws: Agency-Specific

Education

- ORC § 3319.321 – Requires confidentiality of personally identifiable information of any student attending a public school by prohibiting release or access for any unstated purpose.

Health and Human Services

- ORC § 3793.13 – A requirement for the department of alcohol and drug addiction services to maintain as confidential the records or information pertaining to the identity, diagnosis, or treatment of any patient in a drug or alcohol treatment program.

Elections

- ORC § 3503.10 – A confidentiality requirement of voter registration programs to keep the identity of an agency confidential through which a person registered to votes or updated the person's voter registration records, and information relating to a declination to register to vote.

Ohio Privacy Laws: Agency-Specific

Veteran Services

- ORC § 5901.09 – Exempting statements of household income and property from being considered a matter of public record including but not limited to applications for financial assistance.

Bureau of Motor Vehicles

- ORC § 4501.27 – A prohibition from knowingly disclosing or otherwise making available to any person or entity any personal information about an individual that the bureau obtained in connection with a motor vehicle record.

Taxation

- ORC § 5747.18 – Any information gained as a result of returns, investigations, hearings, or verification is confidential and no person shall disclose such information, except for official purposes.

Agenda / Purpose

Good Privacy Practices

Panel Discussion: Privacy and Legal Considerations

Ohio Privacy Laws

Federal Privacy Laws

- Federal Privacy Laws

Fourth Amendment

- The Fourth Amendment of the U.S. Constitution protects individuals from **unreasonable searches and seizures** and requires a **warrant** supported by **probable cause.**
  - Adopted in response to government abuse through the use of general warrants.
  - Subsequent case law (*Katz*) has established that a search has occurred if the government violated an individual's **"reasonable expectation of privacy."**
  - May apply when a government is assessing evidence of illegal activity, e.g., communications stored on a government-issued cell phone or computer
  - *U.S. vs. Warshak* – U.S. Court of Appeals for the Sixth Circuit rules that a person has a reasonable expectation of privacy in emails; government violated Fourth Amendment rights by compelling ISP to turn over emails without first obtaining a warrant based upon probable cause.

Federal – Privacy Laws

DPPA

Health Insurance Portability and Accountability Act

Family Educational Rights and Privacy Act

PRIVACY: RESPECT +PROTECT

OhioDAS Office of Information Technology | Office of Information Security and Privacy

Federal – Privacy Laws

- Drivers Privacy Protection Act (DPPA):
  - Regulates the collection, use and disclosure of motor vehicle records
  - DPPA does not just regulate states – it regulates anyone who obtains, uses or discloses personal data from motor vehicle records.
- Family Educational Rights and Privacy Act (FERPA):
  - Aims to protect the privacy of student education records.
  - FERPA provides parents/guardians or eligible students with the following rights:
    - To review the student's education records
    - To correct any inaccuracies or misleading information in those records
    - To control certain disclosures of the information in those records
    - To file a complaint with the US Department of Education in the event of a violation of the above rights.

PRIVACY: RESPECT +PROTECT

OhioDAS Office of Information Technology | Office of Information Security and Privacy

Federal – Privacy Laws

- The Health Information Portability and Accountability Act (HIPAA):
  - Regulates the privacy and security of medical information.
  - Applies to "covered entities":
    - Health plans
    - Healthcare clearinghouses
    - Healthcare providers
  - Some state agencies or parts of state agencies are considered covered entities
  - Recent changes to HIPAA security and privacy regulations due to the HITECH Act. Contact OISP for more information.

Federal – Privacy Laws

- Fair Credit Reporting Act (FCRA)
  - FCRA governs a consumer reporting agency's creation and disclosure of consumer reports:
    - A consumer reporting agency is "any person which […] regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties […]."
  - Agencies may need to assess where they procure consumer reports
  - HR departments may need to adopt policies and procedures to ensure that consumer reports are properly procured and destroyed
  - Receipts should print no more than the last 5 digits of a credit or debit card or the expiration date.

Federal – Privacy Laws

- U.S. Privacy Act
  - Applies to federal government agencies

BUT

  - Portions may extend to state agencies accessing federal data
    - Social Security Administration data
    - Limitations on use of data
    - Security requirements

Conclusion

- Fair Information Practices Principles
  - Key concepts supporting compliance and standard duty
- Ohio laws
  - Statewide laws such as ORC 1347 apply to all or most
  - Most critical laws deal with your agency specifically
    - Enabling statutes
    - Public records and corresponding exemptions and restrictions
- Federal laws
  - Sector-specific
  - Pre-emption and applicability questions
  - May extend through federal programs

Questions?

PRIVACY: RESPECT +PROTECT

Privacy Trends and Challenges

OhioDAS Office of Information Technology | Office of Information Security and Privacy Service · Support · Solutions

2012

PRIVACY: RESPECT +PROTECT

Agenda / Purpose

Global and Technology Trends

Trends in Public Expectations

Legal Developments

- Trends and Challenges
  - Global and Technology Trends
  - Trends in Public Expectations
  - Legal Developments

OhioDAS Office of Information Technology | Office of Information Security and Privacy

PRIVACY: RESPECT +PROTECT

Agenda / Purpose

Global and Technology Trends

Trends in Public Expectations

Legal Developments

Global and Technology Trends

OhioDAS Office of Information Technology | Office of Information Security and Privacy

PRIVACY: RESPECT +PROTECT

OhioDAS Office of Information Technology | Office of Information Security and Privacy

Identity Theft: Still a Problem

Identity theft reporting system needs improvements, victims say

FTC report outlines identity theft experiences, recommendations

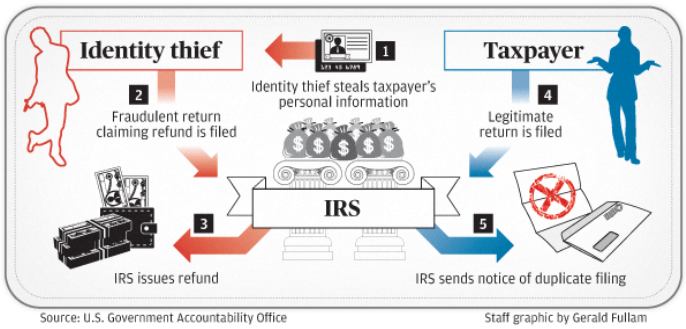
- Government documents/benefits fraud (27%) was the most common form of reported ID theft, followed by credit card fraud (14%)
- Complaints about government documents/benefits fraud increased 11 percentage points since 2009
- 45% of ID theft complainants contacted law enforcement.
- http://www.networkworld.com/news/2012/031312-ftc-identity-theft-257212.html

Identity Theft: Still a Problem

NY ID theft scam has victims in 30 states

How identity theft refund fraud works

In refund fraud, an identity thief uses a taxpayer's name and Social Security number to file for a tax refund, which the IRS discovers only after the legitimate taxpayer files.



Source: U.S. Government Accountability Office

Staff graphic by Gerald Fullam

Data Breaches

- Hacking attacks top list
  - 25.8% of the data breaches recorded in the Identity Theft Resource Center's 2011 Breach Report
  - Five-year high
  - Utah: Data breach affects ~720,000 people
    - April 2012 – Hackers accessed a health department server that didn't have a secure password.
- Data on the Move – 18.1%
- Insider Theft – 13.4 %

PRIVACY: RESPECT +PROTECT

OhioDAS Office of Information Technology | Office of Information Security and Privacy

Hacktivism

Use of unauthorized hacking into computer systems as a form of protest

- Anonymous
  - Has targeted government agencies
  - Will expose data to challenge unsecure systems
- Other examples
  - Wikileaks and Lulzsec

PRIVACY: RESPECT +PROTECT

OhioDAS Office of Information Technology | Office of Information Security and Privacy

On-going Challenges

- Paper records
  - 16% of data breaches recorded in the Identity Theft Resource Center's 2011 Breach Report
  - Potential Harms
    - Maintenance difficulties (Insecurity)
    - Record destruction costs (Insecurity, appropriation, accessibility)
- Unstructured data
  - Sources: database reports, spreadsheets, e-mails, presentations, video
  - Outside scope of ORC 1347.15 but still a concern
- Insider Misuse
  - Intent of ORC 1347.15

Mobile Phones Part 1: BYOD

Privacy Issues

- Protecting State Data
  - Risk of data on easily lost and transferred devices
- Co-mingling and liability of personal data on state IT assets
  - Problematic data within state responsibility
- Employees' privacy risks, rights and expectations
  - 4th amendment implicated?
  - Give notice and choice about risks
  - Accessing data such as geo-location and photos present high-risk in terms of privacy

Related FIPPs – Notice, Choice, Security

Mobile Phones Part 2: Mobile Apps

- Mobile Apps
  - Careful about data collected
  - Minimum necessary
  - Limit retention to that which is necessary
  - Geo-location, contacts and similar types of data are sensitive when collected from apps.

Related FIPPs – Notice, Choice, Security

Social Media

- Potential Problems
  - Inappropriate consumer interaction
    - Via State accounts
    - Oversharing on their part
      - Other people's information
    - Problematic comment on posted information
  - Employee misuse
    - Disclosure of state-maintained PI on personal accounts
  - Employer access to employee accounts
  - Monitoring for comments about agency

Gartner

Gartner Hype Cycle
for Privacy, 2011
(see handout)

All New Technologies

Before using new technologies:

- Privacy impact assessment
- Policy work
- Apply Fair Information Practices Principles
  - Use and Purpose
  - Transparency
  - Participation
  - Integrity, Relevance, Accuracy, Completeness
  - Security
  - Data Minimization
  - Accountability and Auditing

Agenda / Purpose

Global and Technology Trends

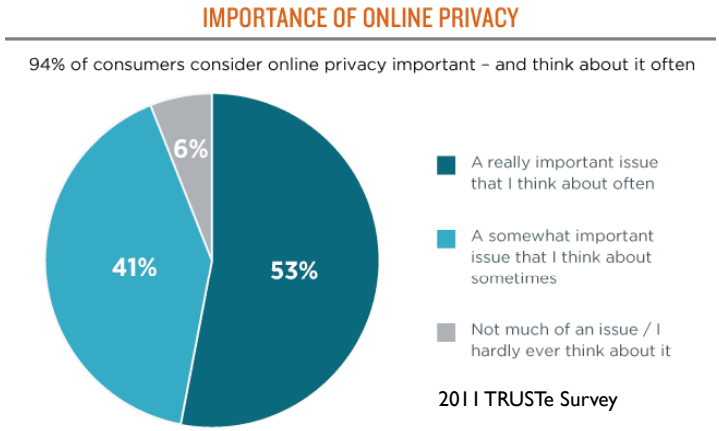
Trends in Public Expectations

Legal Developments

Trends in Public Expectations

Public's Privacy Expectations

- Are we witnessing a privacy "sea change?"



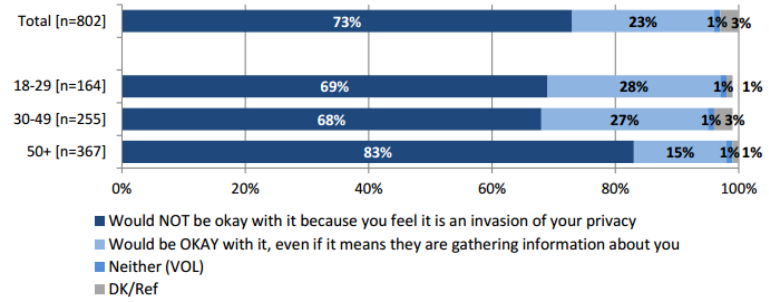
2011 TRUSTe Survey

Public's Privacy Expectations

Three-quarters of search users say collecting user information to personalize search results is not okay

If a search engine kept track of what you search for, and then used that information to personalize your future search results, how would you feel about that?

Based on search users [n=802]

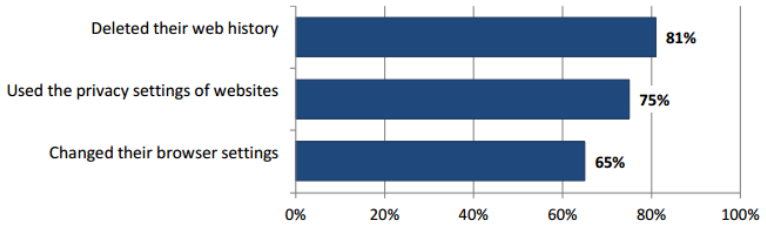


Source: The Pew Research Center's Internet & American Life Project Winter 2012 Tracking Survey, January 20-February 19, 2012. N=2,253 adults, age 18 and older, including 901 cell phone interviews. Interviews conducted in English and Spanish.

Public's Privacy Expectations

Just 38% of online adults say they are aware of ways to limit how much personal information websites can collect about them

The percent of those who are aware of ways to limit information who have done each of the following…



Source: The Pew Research Center's Internet & American Life Project Winter 2012 Tracking Survey, January 20-February 19, 2012. N=2,253 adults, age 18 and older, including 901 cell phone interviews. Interviews conducted in English and Spanish.

Agenda / Purpose

Global and Technology Trends

Trends in Public Expectations

Legal Developments

Legal Developments

Statutory Changes

- In Ohio
  - Additions in 2008 and 2009
  - Since 2009, in specific areas such as public records, health, etc.
  - ?
- Federal law
  - HITECH updates to HIPAA privacy law
    - Security breach notification requirements
    - Pending accounting for disclosures rule
  - Privacy legislation primarily regulating private sector
  - Security breach notification bills
  - Hosts of hearings on privacy issues
    - US DHS and TSA, DOJ, FTC, Google, Apple, Facebook, etc.

Policy Shifts

- U.S. Dept. of Commerce Proposal on Privacy Bill of Rights and "Do not track"
  - Includes a set of principles intended to guide how businesses handle consumers' personal information.
  - Contemplates negotiating a set of practices with industry, consumer protection and privacy advocates and other stakeholders. Practices would be enforceable by FTC.
  - http://www.whitehouse.gov/sites/default/files/email-files/privacy_white_paper.pdf
- Federal Trade Commission also active
  - Policy direction
  - Enforcement
- Potential for same standards to be applied to governments

PRIVACY: RESPECT +PROTECT

OhioDAS Office of Information Technology | Office of Information Security and Privacy

Other Court Cases

- U.S. Supreme Court & Federal Courts
  - 4th Amendment law (*U.S. v. Jones*)
  - Quon (case of accessing texts on a government device used by a government employee)
  - U.S. Privacy Act application
  - Constitutional privacy claims
  - Harms
- Ohio Supreme Court
  - Public records law
    - State ex rel. O'Shea & Assocs. Co., L.P.A. v. Cuyahoga Metro. Hous. Auth. (personal info in question not a "record") January 2012
  - 4th Amendment law

PRIVACY: RESPECT +PROTECT

OhioDAS Office of Information Technology | Office of Information Security and Privacy

Closing Remarks

- Global and Technology Trends
  - Continued rapid change
  - Will continue to create privacy challenges
  - But tech can also enable privacy
- The public:
  - Not abandoned privacy
  - Placing a greater importance on it
- Legal environment
  - Is facing the challenges of this environment
  - Expect new court decisions and new laws pertaining to privacy

Closing Remarks

- Thank you for attending!
- Please complete the survey included in the handouts.

Wrap-Up

Questions and Feedback:

- Daren Arnold, Chief Privacy Officer
  - Daren.Arnold@ohio.gov or 752-7204
- Kevin Brown, Privacy Architect Consultant
  - Kevin.Brown@oit.ohio.gov or 387-5682
- Jillian Burner, Administrative Professional
  - Jillian.Burner@oit.ohio.gov or 644-9391

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 Code[2] 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

Privacy Impact Assessment for the

Project or System Name:

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.

Ohio Privacy Policies Framework

Instructions for Using Privacy Policy and Procedure Templates

The purpose of the Ohio Privacy Policy and Procedure templates is to help state agencies develop a secure and consistent approach to accessing and handling personally identifiable information. Ohio Revised Code 1347.15 requires state agencies to establish administrative rules regulating access to Confidential Personal Information (CPI). Such rules are implemented in agencies through policies and procedures that provide specific guidance on appropriate privacy practices. Furthermore, agencies are likely to have personally identifiable information that is not covered by ORC 1347.15. For these reasons, the accompanying templates serve as a privacy policy and procedure framework for agencies looking to develop or revise their agency's privacy policies and procedures. Use of the templates also helps ensure both ORC 1347.15 compliance and consistent privacy protections to all types of personally identifiable information.

The framework consists of:

- An overarching policy on protecting privacy and all forms of personally identifiable information.
- A procedure for each system containing either CPI or sensitive data.
- Two agency-wide procedures that address: a) notification of improper CPI access and b) handling requests for personally identifiable information.

When your agency's policy development process is complete, you will have established a policy framework similar to that shown in Figure 1:

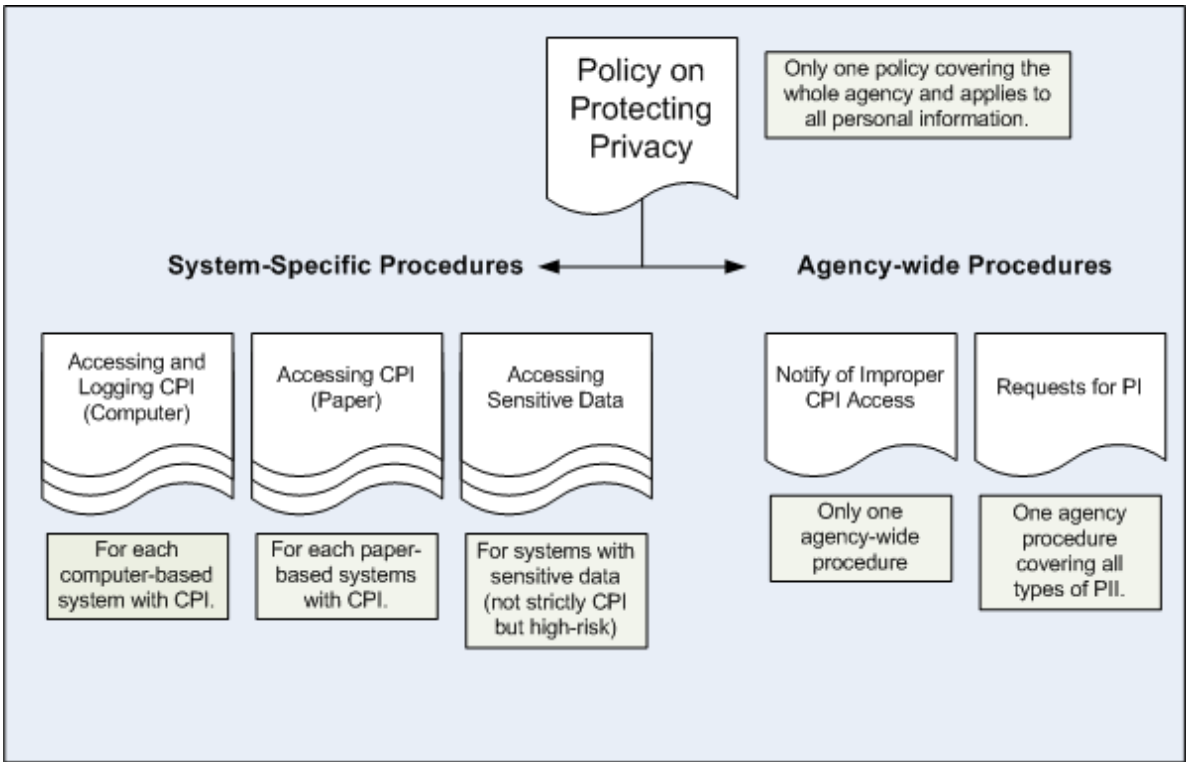


Figure 1: Privacy Policy and Procedure Framework

State agencies are free to use or not use these templates, in whole or in part, although they must still meet the requirements of ORC 1347.15. The templates require a level of customization that reflects the individual agency's data collection practices, appropriate uses, and systems.

To customize the privacy policy and procedure templates to your agency's particular business processes, please use the following instructions as a developmental guide. Note that certain procedures or sections may be unnecessary based on the types of personally identifiable information maintained by your agency.

1. Use any existing documentation. For example, work with the agency's business leaders to obtain an inventory of your agency's information systems, both electronic and paper, that contain sensitive data or CPI. Or, examine the Privacy Impact Assessments for your agency's systems.

2. Using the information in the PIAs, complete a standard operating procedure for each system identified in the inventory. Create one standard operating procedure for each system as follows:

    a. For each electronic system that contains CPI, create a standard operating procedure based on the template, "*Accessing and Logging Confidential Personal Information in a Computer-Based System*." (Use "Template – Accessing and Logging CPI.doc").

    b. For each paper-based system that contains CPI, create a standard operating procedure based on the template "*Accessing Confidential Personal Information in a Paper-Based System*." (Use "Template – Accessing CPI Paper Template.doc").

    c. For each system containing sensitive data that is not within the scope of ORC 1347.15, create a standard operating procedure based on the template "*Accessing Sensitive Data*." (Use "Template – Accessing Sensitive Data.doc"). This procedure is for systems that do not contain CPI but do hold high-risk information that warrants additional precautions.

Once you have completed standard operating procedures for each system that contains sensitive data or CPI within your agency, begin development of the agency-wide ORC 1347.15-related policy and procedures. The Office of Information Security and Privacy recommends that state agencies develop each of the following documents, even if no CPI is maintained by the agency:

3. Create a single, agency-wide standard operating procedure based on the template "*Request to Inspect Personally identifiable Information*." Note that you will need to provide a list of the agency's CPI systems within this standard operating procedure. (Use "Template – Requests for PI.doc").

4. Create a single, agency-wide standard operating procedure based on the template "*Incident Response for Access of Confidential or Sensitive Personal Information for an Invalid Reason."* Note that you will need to provide a list of the agency's CPI systems within this standard operating procedure as well as reference your agency's procedure for security incident response. (Use "Template – SPI-CPI Incident Response.doc").

5. Create a single, agency-wide policy based on the template "*Policy on Protecting Privacy*." This policy will apply to all types of personally identifiable information that the agency maintains. You will need to provide a list of the agency's CPI systems, identify the types of CPI contained in these systems, and reference other agency policies or procedures within this document. (Use "Template – Policy on Protecting Privacy.doc").

These templates and additional resources are available at http://privacy.ohio.gov/Government under "ORC 1347.15 Guidance."

This guidance was developed by the Chief Privacy Officer for the State of Ohio in consultation with the Ohio Privacy Advisory Board. Please contact Office of Information Security and Privacy at (614) 644-9391 or at chief.privacy.officer@oit.ohio.gov if you have any questions about these templates.

Template for "Policy on Protecting Privacy"

11/18/2011

1) See Instructions page for complete information on completing templates.
2) Customize the policy for your agency.
3) Check to ensure that this box and "add information here" type language have been replaced.
4) Place the procedure text into your agency's procedure format, letterhead, etc..

For more information, visit: http://www.privacy.ohio.gov/Government.aspx.

Published by the Office of Information Security and Privacy, a part of the Ohio Department of Administrative Services' Office of Information Technology.

POLICY ON PROTECTING PRIVACY

POLICY NUMBER:	EFFECTIVE DATE:	APPOINTING AUTHORITY APPROVAL:

1. PURPOSE

The *(add agency name here)* takes seriously the protection of personally identifiable information. This policy provides the requirements for protecting the privacy of people who have personally identifiable information in our databases, electronic and paper files and other records. This policy covers all *(add agency name here)* employees. It also covers contractors who gain access to *(add agency name here)* physical facilities or data or computer systems. This policy lays out basic handling expectations first for all types of personally identifiable information, and second, it provides important additional handling requirements for sensitive personally identifiable information.

What is "Personally Identifiable Information" and What is "Sensitive Personally Identifiable Information"?

For the purposes of this policy, "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.

It includes "personal information" as defined by Ohio Revised Code (ORC) 1347.01. Some examples of personally identifiable information are *(add and remove types of personally identifiable information to tailor the list to your agency)*:

- names
- Social Security numbers
- resumes
- correspondence
- addresses
- phone numbers
- driver's license numbers
- state identification numbers
- professional license numbers
- financial account information
- medical and health information
- physical characteristics and other biometric information
- tax information
- education information
- individuals' job classifications and salary information
- performance evaluations
- employment application forms
- timesheets

"Sensitive personally identifiable information" includes personally identifiable information that *(add agency name here)* has discretion not to release under public records law, and it also includes "confidential personal information," which *(add agency name here)* is restricted or prohibited from releasing under Ohio's public records law. Examples of "sensitive personally identifiable information" that *(add agency name here)* keeps includes *(add and remove types of sensitive personally identifiable information to tailor list to your agency)*:

- Social Security numbers
- a person's financial account numbers and information
- beneficiary information
- tax information
- employee voluntary withholdings
- passwords
- employee home addresses and phone numbers
- security challenge questions and answers
- employees' non-state-issued email addresses
- medical and health information
- fingerprints and other biometric information
- driver's license numbers
- state ID card numbers (as issued by the Ohio Bureau of Motor Vehicles)
- confidential personal information (see below)

"Confidential personal information" is personal information that falls within the scope of section 1347.15 of the Revised Code and that *(add agency name here)* is prohibited from releasing under Ohio's public records law. It applies to *(list your agencies confidential personal information here if possible or cross-reference list)* that is maintained in the following *(add number of systems here)* personal information systems only:

- (add system name) – (add division name) (indicate whether system is computer-based or paper-based)

2. POLICY

(Add agency name here) employees and contractors as outlined above must follow these rules on handling all personally identifiable information and handling sensitive personally identifiable information whenever they know or have reason to know that the

information is personally identifiable information or sensitive personally identifiable information.

A. Handling All Personally Identifiable Information

i. Use personally identifiable information only for official, lawful purposes.
ii. Do not access systems with personally identifiable information – whether electronic or paper – if you have not been authorized to do so. Contact your supervisor if you need access.
iii. Enter personally identifiable information accurately. Make a good faith effort to correctly enter data. Never intentionally enter false data.
iv. Take reasonable precautions to protect personally identifiable information from unauthorized modification, destruction, use or disclosure. Follow *(add agency name here)* information security policies and procedures.
v. Whenever an individual requests information that *(add agency name here)* maintains about that individual, employees and contractors shall follow *(add agency name here)* Standard Operating Procedure – Request to Inspect Personally Identifiable Information.
vi. Only collect personally identifiable information when you have been authorized to do so by the proper *(add agency name here)* manager. Do not create an electronic or paper system of record with personally identifiable information unless you have *(add agency name here)* authorization and follow *(add agency name here)*-mandated privacy and security requirements *(or reference named procedure)*.
vii. Destroy personally identifiable information securely in accordance with records retention schedules and following *(add agency name here)* data destruction procedures for particular systems or records *(or reference named procedure)*.
viii. Do not initiate or otherwise contribute to any disciplinary or other punitive action against any individual who reports evidence of unauthorized use of personally identifiable information.
ix. *(Add agency name here)* monitors its information, systems, other IT assets, employees and contractors for compliance with this policy. Therefore, employees and contractors have no expectation of privacy when they use state information, systems and IT assets.

B. Handling Sensitive Personally identifiable information

i. **Only access sensitive personally identifiable information for a valid reason directly related to the exercise of a *(add agency name here)* power or duty.** Valid reasons include *(add reasons specific to your agency's lines of business)*:
   - Responding to a public records request;
   - Responding to a request from an individual for the list of personally identifiable information the agency maintains on that individual;
   - Administering a constitutional provision or duty;
   - Administering a statutory provision or duty;
   - Administering an administrative rule provision or duty;
   - Complying with any state or federal program requirements;
   - Processing or payment of claims or otherwise administering a program with individual participants or beneficiaries;
   - Auditing purposes;

- Carrying out licensure, permit, eligibility, filing, certifications or other similar processes;
- Carrying out or assisting with an authorized investigation or law enforcement purposes;
- Conducting or preparing for administrative hearings;
- Responding to or preparing for litigation, or complying with a court order or subpoena;
- Administering human resources, including but not limited to hiring, promotion, demotion, discharge, salary and compensation issues, leave requests and related issues, time card approvals and related issues;
- Administering an information system;
- Complying with an executive order or policy;
- Complying with an agency policy or a state administrative policy issued by the Department of Administrative Services, the Office of Budget and Management or other similar state agency; or
- Complying with a collective bargaining agreement provision.

ii. **Do not access or use sensitive personally identifiable information for any reason other than those listed above.** For example, do NOT access or use sensitive personally identifiable information:
- for gain or personal profit for yourself or someone else,
- out of simple curiosity or personal interest,
- to commit a crime,
- for retribution, use in a personal conflict, or promotion of a personal point of view, or
- to harass or embarrass.

iii. **You always have a duty not to disclose sensitive personally identifiable information without proper agency authorization.** As you do your work, you may inadvertently or unintentionally come in contact with information that you know or have reason to believe is sensitive personally identifiable information. In those circumstances, you have a duty not to disclose that sensitive personally identifiable information to anyone except properly authorized persons.

iv. **If you suspect that sensitive personally identifiable information has been improperly accessed or disclosed, you shall report the incident to your manager or another manager or contact the *(add agency name here)* Data Privacy Point of Contact at *(add phone number here)***.
- Report quickly and do not disturb evidence.
- Allow the *(add agency name here)* response team to preserve evidence, eliminate any ongoing risks and make a determination that violations have occurred.
- To ensure that any investigation is not compromised and that an accurate evaluation of the incident is conducted, only the director, assistant directors or deputy directors of *(add agency name here)* may authorize notifications to affected individuals.
- Upon a finding that confidential personal information has been access for an invalid reason in violation of a confidentiality statute, section 1347.15 of the Revised Code or rules *(add administrative rule references here)* of the

Administrative Code, the director, assistant directors or deputy directors of *(add agency name here)* will notify affected individuals.

v. Because confidential personal information (CPI) requires a higher standard of care, employees accessing the following **CPI systems** shall follow the privacy procedure specific to that system:
   - See *(add agency name here) (add procedure name here)*.

vi. Nothing in this policy restricts the release of public records. Personally identifiable information is only sensitive if Ohio law gives the agency discretion on its release. Personal information is only confidential if Ohio law prohibits the agency from its release.

3. Violations

i. Any employee who violates this policy is subject to disciplinary action up to and including termination.
ii. Any employee who violates a confidentiality statute or *(add agency name here)* rules *(add administrative rule references here)* is subject to criminal charges, civil liability arising out of the employee's actions, employment termination and a lifelong prohibition against working for the State of Ohio.
iii. Any violation of this policy by a contractor may be considered a material breach of the contract and may subject the contract to termination. Any contractor who violates a confidentiality statute may also be subject to criminal charges and civil liability arising out of the contractor's actions. The vendor may also be subject to vendor debarment.
iv. An employee or contractor who complies in good faith with this policy is not subject to discipline under this policy.
v. This policy does not prohibit an employee from accessing information about himself or herself as long as the person has been granted access to the system and uses authorized processes, or makes a request to *(add agency name here)* for a list of the personally identifiable information that the department maintains about himself or herself.

4. Maintenance of This Policy

This policy will be reviewed at least once annually to ensure that it remains compliant with Federal and State privacy laws including ORC Section 1347.15 and that it accurately reflects *(add agency name here)* personally identifiable information and systems.

5. Questions

For questions regarding this policy, please contact the *(add agency name here)* Data Privacy Point of Contact at *(add phone number here)*.

6. Revision History

Date	Description
MM/DD/YYYY	New policy

[Place on agency letterhead or procedure template]

Template for "Accessing and Logging Confidential Personal Information in a Computer-Based System"

11/18/2011

1) See Instructions page for complete information on completing templates.
2) Customize the procedure for your agency.
3) Check to ensure that this box and "add information here" type language have been replaced.
4) Place the procedure text into your agency's procedure format, letterhead, etc..

For more information, visit: http://www.privacy.ohio.gov/Government.aspx.

Published by the Office of Information Security and Privacy, a part of the Ohio Department of Administrative Services' Office of Information Technology.

Standard Operating Procedure
Accessing and Logging Confidential Personal Information in a Computer-Based System
Insert office name here
Insert name of system here

---

1. Purpose
   This standard operating procedure includes guidance and instructions that must be followed by the employees or contractors of the *(add name of office here)* when accessing Confidential Personal Information contained in *(add name of system here)* which is managed by the *(add name of office here)*.

2. Overview
   All state agencies, boards and commissions are required to implement Ohio Revised Code Section 1347.15 which includes provisions to protect the privacy and security of Ohio's citizens who have confidential personal information stored in a state-maintained personal information system. The *(department name)* has issued administrative rules *(add citation to rules)* regulating access to confidential personal information. This procedure applies those rules to *(add system name here)*.

   For purposes of this procedure:
   - "Personal information," as defined by Ohio Revised Code (ORC) 1347.01, means any information that describes anything about a person, or that indicates actions done by or to a person, or that indicates that a person possesses certain personal characteristics, and that contains, and can be retrieved from a system by, a name, identifying number, symbol, or other identifier assigned to a person.
   - "Confidential personal information" (CPI) is the data identified in section 3. H of this procedure.

[Place on agency letterhead or procedure template]

3. System Description
Note: Complete items A-I below. Add additional items as warranted to provide a full description of this system and the CPI that must be managed.
   A. Name: *provide the name of the system here.*

   B. Description: *provide a description of the system of record here, including an overview of the application used or the platform on which it resides.*

   C. Purpose: *explain why this system is maintained and the purpose it serves.*

   D. Regulatory requirements: *list the citation(s) (state or federal laws or rules) that require or support the existence and maintenance of this system.*

   E. Authorizing access: *explain who authorizes access to the system, how those authorizations are maintained and how those authorizations are revoked when an employee terminates service or otherwise no longer needs access to CPI in the system.*

   F. Security: *explain the security controls that exist with this system such as passwords or other forms of authentication.*

   G. Positions that access the system:

Position title	Permission level (Full access, limited access, etc.)	CPI accessible with this permission level

   H. Description of CPI Contained in this System: *Provide a list of the CPI contained in this system along with the federal or state statutes or administrative rules that make the confidential personal information confidential.*

   I. Valid Reasons for Accessing CPI: *List the valid business reasons as to why this system is used. Be sure to also include the valid reasons for accessing CPI.*

4. Logging Access to Confidential Personal Information

   A. Logging requirements:
   If manual logging is employed, use the attached form to log the following: 1) name (or identifier) of the person whose CPI was accessed and 2) the date. The logging requirement applies whenever access is targeted to a specifically named individual or group of specifically named individuals and does not otherwise come within an exception. In addition, logging is required under the following conditions:

   (Specify the appropriate actions for logging CPI given each of the following scenarios:)

      i. Access in a system containing CPI to accomplish job duties.

      ii. Access in a system containing CPI because of another state employee's request for information.

iii. Public record requests that require accessing a system containing CPI.

B. Manual logging exceptions:
Manual logging is not required under the following conditions:

i. Self service access or request to view own CPI. No logging is necessary when a person views his or her own records containing CPI. For example, an agency customer who makes a request to review his or her case file would not trigger a logging requirement for a caseworker fulfilling the customer's request.

ii. General Research. When conducting general research, employees do not need to log access if the research is not directed toward a specific-named individual or a group of specifically named individuals. For example, running a report that lists licensees licensed from 1996 to 2009 and does not target a specifically named individual is excluded from the logging requirement.

iii. Routine office procedures. Logging is not required when performing routine office tasks that are not directed toward specific individuals or groups of specifically named individuals. For example, running a report that uses parameters other than names, such as dates, without the intention of retrieving the information of a specific employee is excluded from the logging requirement. However, using specific search parameters without a name but with the intent to retrieve a specifically named individual still triggers the logging requirement.

iv. Incidental contact. Logging is not required when an employee incidentally accesses CPI and the contact is merely a result of exposure to the information rather than the primary reason for the access. For example, if a desktop support employee is asked to correct a problem in a system and happens to see CPI because it is already on the screen, the desktop support employee is not required to log access to the CPI because the support employee is not targeting an individual's CPI.

v. Information requested by an individual about that individual. Logging is not required when an individual requests information about that individual. For example, if John Smith requests information on himself, no logging is required. The individual's request for action also serves as the individual's approval to access the information. In addition, "individual" means a natural person, an authorized representative, legal counsel, legal custodian or legal guardian of the individual. Steps should be taken to ensure that the individual is authorized to make the request and has provided credentials for self or to affirm the relationship.

vi. Automated logging. Manual logging is not required when the user's access to CPI is recorded by an automated mechanism. Any upgrade of a system or acquisition of a new system must include an automated recording mechanism. This mechanism shall include:

Application – Name of the application generating the log
Date – The date an event occurred (format should be standardized, such as DD-MM-YYYY or MM-DD-YYYY)
Time – The time the event occurred (HH:MM:SS)
Time Zone – GMT time and offset (if Time not in EST/EDT)
Username – The name of the user accessing the application or attempting to access the application
Person – The name/identifier of the person whose CPI was accessed

C. Use and maintenance of a "Log of Access of Confidential Personal Information": If manual logging is necessary, employees shall use the attached log to list each incident when CPI has been accessed for a specifically named individual or group of specifically named individuals. *(Indicate what information should be captured in the log. Also identify the appropriate security controls for manual CPI logs, e.g., locked file cabinet.*)

D. Retention and destruction of a CPI log: [*Reference the agency's record retention schedule to determine: a) the appropriate length for which CPI logs should be stored and b) the manner in which the logs should be destroyed*].

5. Reporting Suspicious or Inappropriate Requests
Employees are required to immediately report any suspicious or inappropriate actions where it is perceived that CPI may have been requested or accessed for non-business reasons in violations of this procedure or the Policy on Protecting Privacy. See *Incident Response for Access of Confidential or Sensitive Personally Identifiable Information for an Invalid Reason*.

6. Training
A review of this procedure will be included on the agenda of the *(add name of agency routine meeting, e.g., security or ethics)* meetings. In addition, new employees must receive training on this standard operating procedure prior to accessing *(add name of system here)* which contains CPI.

7. Maintenance of this Procedure
This procedure will be reviewed at least once annually to ensure it remains compliant with ORC Section 1347.15 and with any corresponding *(agency)* policy.

8. Revision History

Date	Description
MM/DD/YYYY	New standard operating procedure

[Place on agency letterhead or procedure template]

(add Agency Name here) Log of Access of Confidential Personal Information	
Name of Personal Information System:	
Name of Person Accessing Confidential Personal Information (CPI):	

Acknowledgment: I acknowledge that the information on this log is true and complete and that (check one):

____ I have accessed CPI only for purposes relating to my job duties or my agency's governmental function.

____ I have not knowingly accessed CPI or directed access to CPI that would be logged under the agency Policy on Logging Access to Confidential Personal Information during the following monthly periods: (month/day/year) ___/___/_____ to ___/___/_____.

Initials: _____ Date of Acknowledgement: _____

Check here if this access log contains confidential information: _____

	Name (or identifier) of person whose CPI was accessed	**Date**
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		

[Place on agency letterhead or procedure template]

Template for "Incident Response for Access of Confidential or Sensitive Personally Identifiable Information for an Invalid Reason"

11/18/2011

1) See Instructions page for complete information on completing templates.
2) Customize the procedure for your agency. Make sure that it does not conflict with the agency's IT incident reporting procedure.
3) Check to ensure that this box and "add information here" type language have been replaced.
4) Place the procedure text into your agency's procedure format, letterhead, etc..

For more information, visit: http://www.privacy.ohio.gov/Government.aspx.

Published by the Office of Information Security and Privacy, a part of the Ohio Department of Administrative Services' Office of Information Technology.

Standard Operating Procedure
Incident Response for Access of Confidential or Sensitive Personally Identifiable Information for an Invalid Reason

---

1. Purpose
   This standard operating procedure includes guidance and instructions that must be followed by the employees or contractors of the *(add agency name here)* when Confidential Personal Information (CPI) or Sensitive Personally Identifiable Information (SPII) that is contained in a *(add agency name here)*-managed system is accessed for an invalid reason by a *(add agency name here)* employee or contractor. This document sets forth the procedures for processing illegal activity and wrongdoing, and provides for the careful, expeditious handling of all allegations and claims of improper access. The procedure covers both electronic and paper-based CPI and SPII.

2. Overview
   Ohio Revised Code Section (ORC) 1347.15 (B)(6) requires a state agency to have a procedure to notify each person whose CPI has been accessed for an invalid reason by employees of the state agency. Depending on the circumstances, state and Federal laws require notification of affected individuals when there has been a security breach or invalid access for particular types of PII. However, it is not always clear whether a given incident is in fact a breach or other notification-triggering event. This procedure requires employees and contractors to report incidents so that the agency may make a determination of the steps that need to be taken.

   For purposes of this procedure:

- "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.

  It includes "personal information" as defined by ORC 1347.01. Some examples of personally identifiable information are *(add and remove types of personally identifiable information to tailor the list to your agency)*:
  - names
  - Social Security numbers
  - resumes
  - contracts
  - correspondence
  - addresses
  - phone numbers
  - driver's license numbers
  - state identification numbers
  - professional license numbers
  - financial account information
  - medical and health information
  - physical characteristics and other biometric information
  - education information
  - tax information
  - individuals' job classifications and salary information
  - performance evaluations
  - employment application forms
  - timesheets

- "Sensitive personally identifiable information" includes personally identifiable information that *(add agency name here)* has discretion not to release under public records law, and it also includes "confidential personal information," which *(add agency name here)* is restricted or prohibited from releasing under Ohio's public records law. Examples of "sensitive personally identifiable information" that *(add agency name here)* keeps includes *(add and remove types of SPII to tailor list to your agency)*:
  - Social Security numbers
  - a person's financial account numbers and information
  - beneficiary information
  - tax information
  - employee voluntary withholdings
  - passwords
  - employee home addresses and phone numbers
  - security challenge questions and answers
  - employees' non-state-issued email addresses
  - medical and health information
  - fingerprints and other biometric information
  - driver's license numbers
  - state ID card numbers (as issued by the Ohio Bureau of Motor Vehicles)
  - confidential personal information (see below)

- "Confidential personal information" is personal information that falls within the scope of section 1347.15 of the Revised Code and that *(add agency name here)* is prohibited from releasing under Ohio's public records law. It applies to Social Security numbers, fingerprint data and medical and health information that is maintained in the following *(add number of systems here)* personal information systems only:
  - *(Add system one)*
  - *(Add system two)*

- "Illegal Activity" as used in this procedure includes fraud, theft, assault and other violations of local, state or federal law, including violations of state ethics laws, committed or in the process of being committed, by a state employee on any property owned or leased by the state or during the course of executing official duties.
- The term "incident" refers to facts and circumstances that lead to a reasonable belief that there has been an access of CPI or SPII for an invalid reason that affects one or more computer systems, networks, or other components of the *(add agency name here)* technology infrastructure, or to the threat of such an event.
- "Invalid reason" means any basis for access that is not directly related to *(add agency name here)* exercise of its powers or duties as described in the agency's CPI access policies. Ohio Administrative Code *(add rule reference here)*[1] identifies valid reasons for accessing CPI within the *(add agency name here)*.
- "Wrongdoing" as used in this procedure includes a serious act or omission, committed by a state employee on any property owned or leased by the state or during the course of executing official duties. Wrongdoing is conduct that is not in accordance with standards of proper governmental conduct and which tends to subvert the process of government, including, but not limited, to gross violations of departmental or agency policies and procedures, executive orders, and acts of mismanagement, serious abuses of time, and other serious misconduct. For purposes of this reporting procedure, wrongdoing does not include illegal or suspected illegal activity. Likewise, wrongdoing does not include activity that is most appropriately handled through the department's human resources personnel.

3. Response to access of CPI or SPII for an invalid reason

   A. Responsibilities. *(Add agency name here)* employees and contractors have the following responsibilities when making a report of access of CPI or SPII for an invalid reason:
      a. Employees and contractors shall report incidents of suspected access of CPI or SPII for an invalid reason to a manager. If an employee or contractor is unable to report the suspected incident to a manager, the report should be made to the DPPOC, Chief Legal Counsel or the Administrator for the program area involved.

      b. Managers or the party that received the initial report shall notify the agency Data Privacy Point of Contact (DPPOC) of the suspected incident at (add phone number here).

      c. The DPPOC shall notify the Director that a suspected incident has occurred and will be reviewed. The DPPOC will then coordinate a review of the suspected incident to determine if:
         i. A security breach as defined by ORC 1347.12 has occurred, where "breach" is defined as unauthorized access to computerized data that compromises the security or confidentiality of personal information owned or licensed by a state agency or an agency of a political subdivision and that causes, reasonably is believed to have caused, or reasonably is believed will cause a material risk of identity theft or other fraud to the person or property of a resident of this state.

[1] *(Add URL for administrative rule here)*.

ii. A violation of ORC 1347.15 has occurred, where CPI has been accessed for an invalid reason by an agency employee.
iii. A violation of another regulation, such as the Health Insurance Portability and Accountability Act (HIPAA), has occurred, or that there is some other risk or threat that makes notification of affected parties appropriate.

The DPPOC will involve the following parties in this review:

- Agency human resources representative;
- Agency administrator of the program area involved;
- Agency chief information officer or lead administrator;
- Agency Chief Legal Counsel; and
- Other parties as deemed appropriate.

d. If the review of the suspected incident determines that CPI or SPII has been inappropriately accessed, the Chief Legal Counsel shall report the incident in the following manner:
   - Notify the *(Add agency name here)* Director.
   - Notify the Governor's Office.
   - Notify the Ohio Customer Service and Security Center (OCSSC) at 614-644-0701 or toll free at 800-644-0701.
   - Notify the Ohio State Highway Patrol.

   If there is clear danger and the agency Chief Legal Counsel is not available, the DPPOC can also contact the Ohio State Highway Patrol at 1-877-772-8765.

e. The Deputy Director of the division involved is responsible for notifying all individuals affected by CPI or SPII upon a finding that notification is required or prudent.

f. Employees and contractors should avoid reporting a suspected incident of access to CPI or SPII for an invalid reason to those parties suspected of performing or ordering such access.

g. Although employees are reminded of their duty to comply with the whistleblower statutes ORC 124.341 and ORC 4113.52, employees who report an access of CPI or SPII that they believe is for an invalid reason should have a reasonable factual basis for believing that improper activities have occurred. They should provide as much specific information as possible to allow for proper assessment of the nature, extent, and urgency of the incident.

4. Requests for Incident Information
   If a *(add agency name here)* employee or contractor receives a request for incident information directly from the public, or from any other individual who is not associated with the incident resolution, the *(add agency name here)* employee or contractor will provide no information and will direct the request to the *(add agency name here)* Communications Office, who will coordinate any public statements.

5. Training
   A review of this procedure will be included on the agenda of the *(add name of agency routine meeting, e.g., security or ethics)* meetings. In addition, new employees must receive

training on this standard operating procedure prior to accessing any *(add agency name here)* system that contains CPI.

6. Maintenance of this Procedure
   This procedure will be reviewed at least once annually to ensure it remains compliant with ORC 1347.15 and with any corresponding *(add agency name here)* policy.

7. Revision History

Date	Description
MM/DD/YYYY	New standard operating procedure

[Place on agency letterhead or procedure template]

Template for "Accessing Confidential Personal Information in a Paper-Based System"

11/18/2011

1) See Instructions page for complete information on completing templates.
2) Customize the procedure for your agency.
3) Check to ensure that this box and "add information here" type language have been replaced.
4) Place the procedure text into your agency's procedure format, letterhead, etc..

For more information, visit: http://www.privacy.ohio.gov/Government.aspx.

Published by the Office of Information Security and Privacy, a part of the Ohio Department of Administrative Services' Office of Information Technology.

Standard Operating Procedure
Accessing Confidential Personal Information in a Paper-Based System
Insert office name here
Insert name of system here

---

1. Purpose
   This standard operating procedure includes guidance and instructions that must be followed by the employees or contractors of the *(add name of office here)* when accessing Confidential Personal Information contained in the paper-based system of record, *(add name of system here),* which is managed by the *(add name of office here)*.

2. Overview
   All state agencies, boards and commissions are required to implement Ohio Revised Code Section 1347.15 which includes provisions to protect the privacy and security of Ohio's citizens who have confidential personal information stored in a state-maintained, paper-based personal information system. The *(department name)* has issued administrative rules *(add citation to rules)* regulating access to confidential personal information. This procedure applies those rules to *(add system name here)*.

   For purposes of this procedure:
   - "Personal information," as defined by Ohio Revised Code (ORC) 1347.01, means any information that describes anything about a person, or that indicates actions done by or to a person, or that indicates that a person possesses certain personal characteristics, and that contains, and can be retrieved from a system by, a name, identifying number, symbol, or other identifier assigned to a person.
   - "Confidential personal information" (CPI) is the data identified in section III H of this procedure.

[Place on agency letterhead or procedure template]

3. System Description
Note: Complete items A-I below. Add additional items as warranted to provide a full description of this system and the CPI that must be managed.
   A. Name: *provide the name of the system here.*

   B. Description: *provide a description of the system of record here.*

   C. Purpose: *explain why this system is maintained and the purpose it serves.*

   D. Regulatory requirements: *list the citation(s) (state or federal laws or rules) that require or support the existence and maintenance of this system.*

   E. Authorizing access: *explain who authorizes access to the system, how those authorizations are maintained and how those authorizations are revoked when an employee terminates service or otherwise no longer needs access to CPI in the system.*

   F. Security: *explain the security controls that exist with this system, such as locking mechanisms and the presence of authorized personnel.*

   G. Positions that access the system:

Position title	Permission level (Full access, limited access, etc.)	CPI accessible with this permission level

   H. Description of CPI Contained in this System: *Provide a list of the CPI contained in this system along with the federal or state statutes or administrative rules that make the confidential personal information confidential.*

   I. Valid Reasons for Accessing CPI: *List the valid business reasons as to why this system is used. Be sure to also include the valid reasons for accessing CPI.*

4. Reporting Suspicious or Inappropriate Requests
Employees are required to immediately report any suspicious or inappropriate actions where it is perceived that CPI may have been requested or accessed for non-business reasons in violations of this procedure or the Policy on Protecting Privacy. See *Incident Response for Access of Confidential or Sensitive Personally Identifiable Information for an Invalid Reason*.

5. Training
A review of this procedure will be included on the agenda of the *(add name of agency routine meeting, e.g., security or ethics)* meetings. In addition, new employees must receive training on this standard operating procedure prior to accessing *(add name of system here)* which contains CPI.

6. Maintenance of this Procedure
This procedure will be reviewed at least once annually to ensure it remains compliant with ORC Section 1347.15 and with any corresponding *(agency)* policy.

[Place on agency letterhead or procedure template]

7. Revision History

Date	Description
MM/DD/YYYY	New standard operating procedure

[Place on agency letterhead or procedure template]

Template for "Accessing Sensitive Data"

11/18/2011

1) See Instructions page for complete information on completing templates.
2) Customize the procedure for your agency.
3) Check to ensure that this box and "add information here" type language have been replaced.
4) Place the procedure text into your agency's procedure format, letterhead, etc..

For more information, visit: http://www.privacy.ohio.gov/Government.aspx.

Published by the Office of Information Security and Privacy, a part of the Ohio Department of Administrative Services' Office of Information Technology.

Standard Operating Procedure
Accessing Sensitive Data
Insert office name here
Insert name of system here

---

1. Purpose
   This standard operating procedure includes guidance and instructions that must be followed by the employees or contractors of the *(add office name here)* when accessing sensitive data contained in the *(add system name here)* which is managed by the *(add office name here)*.

2. Overview
   This procedure only addresses the access of sensitive data, which may include sensitive personally identifiable information (SPII). For purposes of this procedure:
   - "Sensitive data" is the data identified in section 3 H of this procedure.
   - "Sensitive personally identifiable information" includes personally identifiable information that *(add agency name here)* has discretion not to release under public records law. For purposes of this procedure, it does not include "confidential personal information" under Ohio Revised Code 1347.15. Examples of "sensitive personally identifiable information" that *(add agency name here)* keeps may include *(add and remove types of sensitive personally identifiable information to tailor list to your agency)*:

- Social Security numbers
- a person's financial account numbers and information
- beneficiary information
- tax information
- employee voluntary withholdings
- passwords
- employee home addresses and phone numbers
- security challenge questions and answers
- employees' non-state-issued email addresses
- medical and health information
- fingerprints and other biometric information
- driver's license numbers
- state ID card numbers (as issued by the Ohio Bureau of Motor Vehicles)
- confidential personal information

3. System Description
   Note: Complete items A-I below. Add additional items as warranted to provide a full description of this system and the sensitive data that must be managed.
   A. Name: *provide the name of the system here.*

   B. Description: *provide the technical description of the system here, including the application used or the platform on which it resides.*

   C. Purpose: *explain why this system is maintained and the purpose it serves.*

   D. Regulatory requirements: *list the citation(s) (state or federal laws or rules) that require the existence and maintenance of this system.*

   E. Authorizing access: *explain who authorizes access to the system, how those authorizations are maintained and how those authorizations are revoked when an employee terminates service.*

   F. Security: *explain the security permissions that exist with this system such as passwords or other forms of authentication.*

   G. Positions that access the system:

Position title	Permission level (Full access, limited access, etc.)	Sensitive data accessible with this permission level

   H. Description of Sensitive Data Contained in this System: *Provide a list of the sensitive data contained in this system.*

   I. Valid Reasons for Accessing Sensitive Data: *List the valid business reasons as to why this system is used. Be sure to also include the valid reasons for accessing sensitive data.*

4. Reporting Suspicious or Inappropriate Requests
   Employees are required to immediately report any suspicious or inappropriate actions where it is perceived that sensitive data may have been requested or accessed for non-business reasons in violations of this procedure or the Policy on Protecting Privacy. See *IT Policy (insert policy number here), "Security Incident Response."*

5. Training
   A review of this procedure will be included on the agenda of the *(add name of agency routine meeting, e.g., security or ethics)* meetings. In addition, new employees must receive training on this standard operating procedure prior to accessing the *(add system name here)* which contains sensitive data.

6. Maintenance of this Procedure

This procedure will be reviewed at least once annually to ensure it remains compliant with Ohio law and with any corresponding *(insert agency name)* policy.

7. Revision History

Date	Description
MM/DD/YYYY	New standard operating procedure

[Place on agency letterhead or procedure template]

Template for "Request to Inspect Personal Information"

11/18/2011

1) See Instructions page for complete information on completing templates.
2) Customize the procedure for your agency.
3) Check to ensure that this box and "add information here" type language have been replaced.
4) Place the procedure text into your agency's procedure format, letterhead, etc..

For more information, visit: http://www.privacy.ohio.gov/Government.aspx.

Published by the Office of Information Security and Privacy, a part of the Ohio Department of Administrative Services' Office of Information Technology.

Standard Operating Procedure
Request to Inspect Personal Information

---

1. Purpose
   This standard operating procedure includes guidance and instructions that must be followed by the employees or contractors of the *(add agency name here)* when responding to written requests to inspect Personal Information (PI) contained in a system managed by *(add agency name here)*.

2. Overview
   In accordance with Ohio Revised Code (ORC) 1347.08(A), upon the request of a properly identified person, every state agency that maintains a personal information system must:

   - inform that person of the existence of any personal information about him or her in the system;
   - permit the person to inspect that personal information in the system(s); and
   - inform the person about the types of uses made of the personal information and the identity of users granted accessed.

   Exceptions to ORC 1347.08 also exist and must be considered.

   ORC Section 1347.15(B)(5) requires state agencies to comply with a written request from an individual for a list of Confidential Personal Information (CPI) about the individual that the state agency keeps, unless the CPI relates to an investigation about the individual based upon specific statutory authority by the state agency.

   "Individual" means a natural person, an authorized representative, legal counsel, legal custodian or legal guardian of the individual.

"Personal information," as defined by Ohio Revised Code (ORC) 1347.01, means any information that describes anything about a person, or that indicates actions done by or to a person, or that indicates that a person possesses certain personal characteristics, and that contains, and can be retrieved from a system by, a name, identifying number, symbol, or other identifier assigned to a person. Some examples of personal information are:

- names
- Social Security numbers
- resumes
- contracts
- correspondence
- addresses
- phone numbers
- driver's license numbers
- state identification numbers
- professional license numbers
- financial account information
- medical and health information
- physical characteristics and other biometric information
- education information
- tax information
- individuals' job classifications and salary information
- performance evaluations
- employment application forms
- timesheet

"Sensitive personally identifiable information" includes personally identifiable information that *(add agency name here)* has discretion not to release under public records law, and it also includes "confidential personal information," which *(add agency name here)* is restricted or prohibited from releasing under Ohio's public records law. Examples of "sensitive personally identifiable information" that *(add agency name here)* keeps includes *(add and remove types of sensitive personally identifiable information to tailor list to your agency)*:

- Social Security numbers
- a person's financial account numbers and information
- beneficiary information
- tax information
- employee voluntary withholdings
- passwords
- employee home addresses and phone numbers
- security challenge questions and answers
- employees' non-state-issued email addresses
- medical and health information
- fingerprints and other biometric information
- driver's license numbers
- state ID card numbers (as issued by the Ohio Bureau of Motor Vehicles)
- confidential personal information (see below)

"Confidential personal information" is personal information that falls within the scope of section 1347.15 of the Revised Code and that *(add agency name here)* is prohibited from releasing under Ohio's public records law. It applies to Social Security numbers, fingerprint data and medical and health information that is maintained in the following *(add number of systems here)* personal information systems only:

- *(add system name here)– (add division name here) (indicate whether system is computer-based or paper-based)*

3. <u>Requests to Inspect Personal Information</u>

   A. <u>Evaluate the Request</u>:

As a standard practice, general requests from individuals to review their own personal information should be routed to the appropriate *(add agency name here)* division records manager for evaluation. The requester must put the request for personal information in writing. Individual *(add agency name here)* offices may have specific business processes that involve the collection, verification or communication with customers regarding their personal information. This procedure does not supersede those business processes as long as those business processes are consistent with chapter 1347 of the Revised Code in providing individuals with an opportunity to review their personal information.

B. Verify the Identity of the Requester

If the personal information entirely constitutes a public record subject to disclosure under ORC 149.43, then it will be disclosed in accordance with *(add agency policy reference here)*. For personal information that is not a public record, however, the subject of the information still has a right, with some limitations, to review his or her own information under ORC Chapter 1347.

If the information requested constitutes sensitive personally identifiable information, then the law may give *(add agency name here)* the discretion in releasing the information to the public in general. If the personal information constitutes CPI, then the law prohibits the agency from releasing the information except to certain parties. *For this reason, the records manager must verify the identity of the requester of sensitive or confidential personal information to ensure that fulfilling the request for those types of personal information is appropriate.* To verify the requester's identity, the requester must appear in person and present a valid driver's license, official state identification card or passport. In the event an individual cannot present one of those three photo IDs, the department may accept a similarly trustworthy form of verification. Use of an alternative form of verification shall be approved by a deputy director prior to release the sensitive or confidential personal information.

C. Limitations on Disclosure

The records manager must notify the *(add agency legal office name here)* of each request for personal inspection of sensitive or confidential personal information. The records manager, in consultation with the *(add agency legal office name here)*, must determine if there are any requirements pertaining to the disclosure of the personal information or any legal restriction that limits the release of personal information to the subject of the information. Some examples include:

- *(Add agency name here)* is not required to release any confidential personal information under ORC 1347.15 that relates to an investigation about that individual.
- The records manager, in consultation with the *(add agency legal office name here)*, must disclose medical, psychiatric, or psychological information to a person who is the subject of the information or to the person's legal guardian, unless a physician, psychiatrist, or psychologist determines for the agency that the disclosure of the information is likely to have an adverse effect on the person. In this case, the information shall be released to a physician, psychiatrist, or psychologist who is designated by the person or by the person's legal guardian.
- *(Add agency name here)* must not release a confidential law enforcement investigatory record or trial preparation record as defined in divisions (A)(2) and (4) of section 149.43 of the Revised Code.

- *(Add agency name here)* is not required to release any personal information about an individual if the information is excluded from the scope of Chapter 1347 of the Revised Code.

D. Dispose the Request
Personal information is to be available for inspection during regular business hours, with the exception of published holidays. Personal information must be made available for inspection promptly. Copies of personal information must be made available within a reasonable period of time. “Prompt” and “reasonable” take into account the volume of personal information requested; the proximity of the location where the information is stored; and the necessity for any legal review of the information requested.

Each request should be evaluated for an estimated length of time required to gather the personal information. All requests for personal information must be satisfied within a reasonable time. Requests for personal information should be coordinated with the *(add agency communications office name here)* and the *(add agency legal office name here)*.

4. Costs for Personal Information.
Those seeking personal information will be charged only the actual cost of making copies.
   - The standard charge for paper copies is 5 cents per page.
   - The charge for computer files placed on a compact disc is $1 per disc.

   Requesters may ask that records be mailed to them. Electronic sensitive personally identifiable information shall be sent to the requester in an encrypted format. The means of decrypting the information shall be sent through a separate communication. They will be charged the actual cost of the postage and mailing supplies. The office may require the requester to pay the cost of providing the information in advance.

5. Questions
For questions regarding this policy, please contact the *(add agency legal office name here)* at *(add phone number here)*.

6. Maintenance of this Procedure
This procedure will be reviewed at least once annually to ensure it remains compliant with ORC Sections 1347.08 and 1347.15 and with any corresponding *(add agency name here)* policy.

7. Revision History

Date	Description
MM/DD/YYYY	New standard operating procedure

Role of the Data Privacy Point of Contact

Each state agency is required by Ohio Revised Code 1347.15(B)(7) to appoint a Data Privacy Point of Contact (DPPOC):

> [...] the director of the state agency [shall] designate an employee of the state agency to serve as the data privacy point of contact within the state agency to work with the chief privacy officer within the office of information technology to ensure that confidential personal information is properly protected and that the state agency complies with this section and rules adopted thereunder;

Who should be the DPPOC within your agency and what does the DPPOC do? Below are some answers to potential questions about the DPPOC position.

Your agency has to have one. Why not put it to good use?

Robust privacy practices build trust with customers and employees in addition to enhancing an agency's reputation. Good privacy is good government – no matter the nature of the agency. An internal privacy adviser, familiar with the business as well as with privacy law adds value to the agency and all of its components.

An empowered DPPOC can help prevent problems from arising. This saves expense and maintains the public's trust in the agency. If someone complains that the agency has breached their privacy, the DPPOC can handle things quickly and effectively. This is particularly important because agencies usually have an ongoing relationship with the person (for example, a customer or an employee). Again, this can save money and time. Thus, a privacy coordinator is not only required by law but an invaluable asset for agencies.

What does a DPPOC do?

A DPPOC:

- is familiar with any other legislation governing the agency's responsibilities and limits in regards to personal information;
- is familiar with Chapter 1347 of the Ohio Revised Code, "Personal Information Systems";
- works to address inquiries and complaints from the agency's clients about privacy matters;

- coordinates privacy impact assessments for the agency
- trains other staff at the agency on good privacy practices;
- advises managers on how to ensure the agency's business practices comply with privacy requirements;
- advises managers on the privacy impacts (if any) of changes to the agency's business practices and information systems;
- advises managers if improving privacy practices might improve the business;
- coordinates requests for access to personal information, or correction of personal information; and
- acts as a liaison for the agency with the State Chief Privacy Officer. This is particularly important if the agency is responding to a possible privacy breach. The Chief Privacy Officer also regularly e-mails the DPPOC network with privacy-related news and guidance.

Who should serve as the DPPOC?

The DPPOC is a multi-disciplinary role, and so a successful DPPOC needs to have the knowledge and capability to coordinate issues involving legal, IT and the business units. With regard to other key characteristics, a DPPOC is someone who:

- Understands the type of information the agency collects and it works with the agency's key business processes and systems;
- Understands the legal basis for the agency collecting, using and sharing personal information;
- Is capable enough with legal concepts to understand the privacy laws that regulate the agency;
- Has a degree of comfort with technology to understand how information is used and flows to, from and throughout the agency.
- Is sufficiently positioned to advocate appropriate solutions to address risks to individuals (harms from improper disclosure or use) and to the agency (lack of legal compliance and loss of public trust).
- Has support from senior leadership.

This depends on the size of the agency, the responsibilities of the agency, and the type of personal information it handles. For example:

- In a small agency, like a small business, the overall manager will often is responsible for legal compliance requirements, including privacy in addition to labor, equal opportunity, ethics, etc. An existing staff member might be asked to advise the manager or managers on privacy issues.
- If the agency has an in-house lawyer, that person is sometimes the DPPOC, particularly those agencies with significant privacy regulations.
- Sometimes, an agency IT administrator or information security officer will also serve as a data privacy point of contact.
- In large agencies or agencies that handle a lot of personal information, there may be a need for one or more employees focusing exclusively on privacy matters.

In the end specific qualifications do not matter as much as having a DPPOC upon whom other managers can rely as a resource for privacy issues.

Training and help for DPPOCs

The Office of Information Security and Privacy is available to assist DPPOCs.

- We offer privacy leadership training sessions each year.
- Our staff can answer general questions about how certain privacy laws works. We cannot provide legal advice on particular problems, but we may be able to suggest someone and resources that can help.
- **Communicate agency privacy concerns to the Chief Privacy Officer**: Please help ensure that the Chief Privacy Officer is aware of privacy-related issues within your agency. The Office of Information Security & Privacy has a number of resources that may help you address a privacy problem. Also, if a number of agencies experience the same problem, an opportunity for an enterprise approach may apply.
- **Please submit contact information for your agency data privacy point of contact to the Office of Information Security and Privacy.**

  Contact us at chief.privacy.officer@oit.ohio.gov or (614) 387-0320 if you think we may be of assistance.

OHIO REVISED CODE

Chapter 1347: PERSONAL INFORMATION SYSTEMS

ORC 1347.01 Personal information systems definitions.

As used in this chapter, except as otherwise provided:

(A) "State agency" means the office of any elected state officer and any agency, board, commission, department, division, or educational institution of the state.

(B) "Local agency" means any municipal corporation, school district, special purpose district, or township of the state or any elected officer or board, bureau, commission, department, division, institution, or instrumentality of a county.

(C) "Special purpose district" means any geographic or political jurisdiction that is created by statute to perform a limited and specific function, and includes, but is not limited to, library districts, conservancy districts, metropolitan housing authorities, park districts, port authorities, regional airport authorities, regional transit authorities, regional water and sewer districts, sanitary districts, soil and water conservation districts, and regional planning agencies.

(D) "Maintains" means state or local agency ownership of, control over, responsibility for, or accountability for systems and includes, but is not limited to, state or local agency depositing of information with a data processing center for storage, processing, or dissemination. An agency "maintains" all systems of records that are required by law to be kept by the agency.

(E) "Personal information" means any information that describes anything about a person, or that indicates actions done by or to a person, or that indicates that a person possesses certain personal characteristics, and that contains, and can be retrieved from a system by, a name, identifying number, symbol, or other identifier assigned to a person.

(F) "System" means any collection or group of related records that are kept in an organized manner and that are maintained by a state or local agency, and from which personal information is retrieved by the name of the person or by some identifying number, symbol, or other identifier assigned to the person. "System" includes both records that are manually stored and records that are stored using electronic data processing equipment. "System" does not include collected archival records in the custody of or administered under the authority of the Ohio historical society, published directories, reference materials or newsletters, or routine information that is maintained for the purpose of internal office administration, the use of which would not adversely affect a person.

(G) "Interconnection of systems" means a linking of systems that belong to more than one agency, or to an agency and other organizations, which linking of systems results in a system that permits each agency or organization involved in the linking to have unrestricted access to the systems of the other agencies and organizations.

(H) "Combination of systems" means a unification of systems that belong to more than one agency, or to an agency and another organization, into a single system in which the records that belong to each agency or organization may or may not be obtainable by the others.

ORC 1347.04 Exemptions from chapter.

(A)(1) Except as provided in division (A)(2) of this section or division (C)(2) of section 1347.08 of the Revised Code, the following are exempt from the provisions of this chapter:

(a) Any state or local agency, or part of a state or local agency, that performs as its principal function any activity relating to the enforcement of the criminal laws, including police efforts to prevent, control, or reduce crime or to apprehend criminals;

(b) The criminal courts;

(c) Prosecutors;

(d) Any state or local agency or part of any state or local agency that is a correction, probation, pardon, or parole authority;

(e) Personal information systems that are comprised of investigatory material compiled for law enforcement purposes by agencies that are not described in divisions (A)(1)(a) and (d) of this section.

(2) A part of a state or local agency that does not perform, as its principal function, an activity relating to the enforcement of the criminal laws is not exempt under this section.

(B) The provisions of this chapter shall not be construed to prohibit the release of public records, or the disclosure of personal information in public records, as defined in section 149.43 of the Revised Code, or to authorize a public body to hold an executive session for the discussion of personal information if the executive session is not authorized under division (G) of section 121.22 of the Revised Code.

The disclosure to members of the general public of personal information contained in a public record, as defined in section 149.43 of the Revised Code, is not an improper use of personal information under this chapter.

(C) The provisions of this chapter shall not be construed to prohibit, and do not prohibit, compliance with any order issued pursuant to division (D)(1) of section 2151.14 of the Revised Code, any request for records that is properly made pursuant to division (D)(3)(a) of section 2151.14 or division (A) of section 2151.141 of

the Revised Code, or any determination that is made by a court pursuant to division (D)(3)(b) of section 2151.14 or division (B)(1) of section 2151.141 of the Revised Code.

ORC 1347.05 Duties of state and local agencies maintaining personal information systems.

Every state or local agency that maintains a personal information system shall:

(A) Appoint one individual to be directly responsible for the system;

(B) Adopt and implement rules that provide for the operation of the system in accordance with the provisions of this chapter that, in the case of state agencies, apply to state agencies or, in the case of local agencies, apply to local agencies;

(C) Inform each of its employees who has any responsibility for the operation or maintenance of the system, or for the use of personal information maintained in the system, of the applicable provisions of this chapter and of all rules adopted in accordance with this section;

(D) Specify disciplinary measures to be applied to any employee who initiates or otherwise contributes to any disciplinary or other punitive action against any individual who brings to the attention of appropriate authorities, the press, or any member of the public, evidence of unauthorized use of information contained in the system;

(E) Inform a person who is asked to supply personal information for a system whether the person is legally required to, or may refuse to, supply the information;

(F) Develop procedures for purposes of monitoring the accuracy, relevance, timeliness, and completeness of the personal information in this system, and, in accordance with the procedures, maintain the personal information in the system with the accuracy, relevance, timeliness, and completeness that is necessary to assure fairness in any determination made with respect to a person on the basis of the information;

(G) Take reasonable precautions to protect personal information in the system from unauthorized modification, destruction, use, or disclosure;

(H) Collect, maintain, and use only personal information that is necessary and relevant to the functions that the agency is required or authorized to perform by statute, ordinance, code, or rule, and eliminate personal information from the system when it is no longer necessary and relevant to those functions.

ORC 1347.06 Administrative rules.

The director of administrative services shall adopt, amend, and rescind rules pursuant to Chapter 119. of the Revised Code for the purposes of administering and enforcing the provisions of this chapter that pertain to state agencies.

A state or local agency that, or an officer or employee of a state or local agency who, complies in good faith with a rule applicable to the agency is not subject to criminal prosecution or civil liability under this chapter.

ORC 1347.07 Using personal information.

A state or local agency shall only use the personal information in a personal information system in a manner that is consistent with the purposes of the system.

ORC 1347.071 Placing or using information in interconnected or combined systems.

(A) No state or local agency shall place personal information in an interconnected or combined system, or use personal information that is placed in an interconnected or combined system by another state or local agency or another organization, unless the interconnected or combined system will contribute to the efficiency of the involved agencies in implementing programs that are authorized by law.

(B) No state or local agency shall use personal information that is placed in an interconnected or combined system by another state or local agency or another organization, unless the personal information is necessary and relevant to the performance of a lawful function of the agency.

(C) When a state or local agency requests a person to supply personal information that will be placed in an interconnected or combined system, the agency shall provide the person with information relevant to the system, including the identity of the other agencies or organizations that have access to the information in the system.

ORC 1347.08 Rights of person who are subject of personal information.

(A) Every state or local agency that maintains a personal information system, upon the request and the proper identification of any person who is the subject of personal information in the system, shall:

(1) Inform the person of the existence of any personal information in the system of which the person is the subject;

(2) Except as provided in divisions (C) and (E)(2) of this section, permit the person, the person's legal guardian, or an attorney who presents a signed written authorization made by the person, to inspect all personal information in the system of which the person is the subject;

(3) Inform the person about the types of uses made of the personal information, including the identity of any users usually granted access to the system.

(B) Any person who wishes to exercise a right provided by this section may be accompanied by another individual of the person's choice.

(C)(1) A state or local agency, upon request, shall disclose medical, psychiatric, or psychological information to a person who is the subject of the information or to the person's legal guardian, unless a physician, psychiatrist, or psychologist determines for the agency that the disclosure of the information is likely to have an adverse effect on the person, in which case the information shall be released to a physician, psychiatrist, or psychologist who is designated by the person or by the person's legal guardian.

(2) Upon the signed written request of either a licensed attorney at law or a licensed physician designated by the inmate, together with the signed written request of an inmate of a correctional institution under the administration of the department of rehabilitation and correction, the department shall disclose medical information to the designated attorney or physician as provided in division (C) of section 5120.21 of the Revised Code.

(D) If an individual who is authorized to inspect personal information that is maintained in a personal information system requests the state or local agency that maintains the system to provide a copy of any personal information that the individual is authorized to inspect, the agency shall provide a copy of the personal information to the individual. Each state and local agency may establish reasonable fees for the service of copying, upon request, personal information that is maintained by the agency.

(E)(1) This section regulates access to personal information that is maintained in a personal information system by persons who are the subject of the information, but does not limit the authority of any person, including a person who is the subject of personal information maintained in a personal information system, to inspect or have copied, pursuant to section 149.43 of the Revised Code, a public record as defined in that section.

(2) This section does not provide a person who is the subject of personal information maintained in a personal information system, the person's legal guardian, or an attorney authorized by the person, with a right to inspect or have copied, or require an agency that maintains a personal information system to permit the inspection of or to copy, a confidential law enforcement investigatory record or trial preparation record, as defined in divisions (A)(2) and (4) of section 149.43 of the Revised Code.

(F) This section does not apply to any of the following:

(1) The contents of an adoption file maintained by the department of health under section 3705.12 of the Revised Code;

(2) Information contained in the putative father registry established by section 3107.062 of the Revised Code, regardless of whether the information is held by the department of job and family services or, pursuant to section 3111.69 of the Revised Code, the office of child support in the department or a child support enforcement agency;

(3) Papers, records, and books that pertain to an adoption and that are subject to inspection in accordance with section 3107.17 of the Revised Code;

(4) Records listed in division (A) of section 3107.42 of the Revised Code or specified in division (A) of section 3107.52 of the Revised Code;

(5) Records that identify an individual described in division (A)(1) of section 3721.031 of the Revised Code, or that would tend to identify such an individual;

(6) Files and records that have been expunged under division (D)(1) or (2) of section 3721.23 of the Revised Code;

(7) Records that identify an individual described in division (A)(1) of section 3721.25 of the Revised Code, or that would tend to identify such an individual;

(8) Records that identify an individual described in division (A)(1) of section 5111.61 of the Revised Code, or that would tend to identify such an individual;

(9) Test materials, examinations, or evaluation tools used in an examination for licensure as a nursing home administrator that the board of examiners of nursing home administrators administers under section 4751.04 of the Revised Code or contracts under that section with a private or government entity to administer;

(10) Information contained in a database established and maintained pursuant to section 5101.13 of the Revised Code.

ORC 1347.09 Disputing information.

(A)(1) If any person disputes the accuracy, relevance, timeliness, or completeness of personal information that pertains to him and that is maintained by any state or local agency in a personal information system, he may request the agency to investigate the current status of the information. The agency shall, within a reasonable time after, but not later than ninety days after, receiving the request from the disputant, make a reasonable investigation to determine whether the disputed information is accurate, relevant, timely, and complete, and shall notify the disputant of the results of the investigation and of the action that the agency plans to take with respect to the disputed information. The agency shall delete any information that it cannot verify or that it finds to be inaccurate.

(2) If after an agency's determination, the disputant is not satisfied, the agency shall do either of the following:

(a) Permit the disputant to include within the system a brief statement of his position on the disputed information. The agency may limit the statement to not more than one hundred words if the agency assists the disputant to write a clear summary of the dispute.

(b) Permit the disputant to include within the system a notation that the disputant protests that the information is inaccurate, irrelevant, outdated, or incomplete. The agency shall maintain a copy of

the disputant's statement of the dispute. The agency may limit the statement to not more than one hundred words if the agency assists the disputant to write a clear summary of the dispute.

(3) The agency shall include the statement or notation in any subsequent transfer, report, or dissemination of the disputed information and may include with the statement or notation of the disputant a statement by the agency that it has reasonable grounds to believe that the dispute is frivolous or irrelevant, and of the reasons for its belief.

(B) The presence of contradictory information in the disputant's file does not alone constitute reasonable grounds to believe that the dispute is frivolous or irrelevant.

(C) Following any deletion of information that is found to be inaccurate or the accuracy of which can no longer be verified, or if a statement of dispute was filed by the disputant, the agency shall, at the written request of the disputant, furnish notification that the information has been deleted, or furnish a copy of the disputant's statement of the dispute, to any person specifically designated by the person. The agency shall clearly and conspicuously disclose to the disputant that he has the right to make such a request to the agency.

ORC 1347.10 Wrongful disclosure.

(A) A person who is harmed by the use of personal information that relates to him and that is maintained in a personal information system may recover damages in civil action from any person who directly and proximately caused the harm by doing any of the following:

(1) Intentionally maintaining personal information that he knows, or has reason to know, is inaccurate, irrelevant, no longer timely, or incomplete and may result in such harm;

(2) Intentionally using or disclosing the personal information in a manner prohibited by law;

(3) Intentionally supplying personal information for storage in, or using or disclosing personal information maintained in, a personal information system, that he knows, or has reason to know, is false;

(4) Intentionally denying to the person the right to inspect and dispute the personal information at a time when inspection or correction might have prevented the harm.

An action under this division shall be brought within two years after the cause of action accrued or within six months after the wrongdoing is discovered, whichever is later; provided that no action shall be brought later than six years after the cause of action accrued. The cause of action accrues at the time that the wrongdoing occurs.

(B) Any person who, or any state or local agency that, violates or proposes to violate any provision of this chapter may be enjoined by any court of competent jurisdiction. The court may issue an order or enter a

judgment that is necessary to ensure compliance with the applicable provisions of this chapter or to prevent the use of any practice that violates this chapter. An action for an injunction may be prosecuted by the person who is the subject of the violation, by the attorney general, or by any prosecuting attorney.

ORC 1347.12 Agency disclosure of security breach of computerized personal information data.

(A) As used in this section:

(1) "Agency of a political subdivision" means each organized body, office, or agency established by a political subdivision for the exercise of any function of the political subdivision, except that "agency of a political subdivision" does not include an agency that is a covered entity as defined in 45 C.F.R. 160.103, as amended.

(2)(a) "Breach of the security of the system" means unauthorized access to and acquisition of computerized data that compromises the security or confidentiality of personal information owned or licensed by a state agency or an agency of a political subdivision and that causes, reasonably is believed to have caused, or reasonably is believed will cause a material risk of identity theft or other fraud to the person or property of a resident of this state.

(b) For purposes of division (A)(2)(a) of this section:

(i) Good faith acquisition of personal information by an employee or agent of the state agency or agency of the political subdivision for the purposes of the agency is not a breach of the security of the system, provided that the personal information is not used for an unlawful purpose or subject to further unauthorized disclosure.

(ii) Acquisition of personal information pursuant to a search warrant, subpoena, or other court order, or pursuant to a subpoena, order, or duty of a regulatory state agency, is not a breach of the security of the system.

(3) "Consumer reporting agency that compiles and maintains files on consumers on a nationwide basis" means a consumer reporting agency that regularly engages in the practice of assembling or evaluating, and maintaining, for the purpose of furnishing consumer reports to third parties bearing on a consumer's creditworthiness, credit standing, or credit capacity, each of the following regarding consumers residing nationwide:

(a) Public record information;

(b) Credit account information from persons who furnish that information regularly and in the ordinary course of business.

(4) "Encryption" means the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

(5) "Individual" means a natural person.

(6)(a) "Personal information" means, notwithstanding section 1347.01 of the Revised Code, an individual's name, consisting of the individual's first name or first initial and last name, in combination with and linked to any one or more of the following data elements, when the data elements are not encrypted, redacted, or altered by any method or technology in such a manner that the data elements are unreadable:

(i) Social security number;

(ii) Driver's license number or state identification card number;

(iii) Account number or credit or debit card number, in combination with and linked to any required security code, access code, or password that would permit access to an individual's financial account.

(b) "Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records or any of the following media that are widely distributed:

(i) Any news, editorial, or advertising statement published in any bona fide newspaper, journal, or magazine, or broadcast over radio or television;

(ii) Any gathering or furnishing of information or news by any bona fide reporter, correspondent, or news bureau to news media described in division (A)(6)(b)(i) of this section;

(iii) Any publication designed for and distributed to members of any bona fide association or charitable or fraternal nonprofit corporation;

(iv) Any type of media similar in nature to any item, entity, or activity identified in division (A)(6)(b)(i), (ii), or (iii) of this section.

(7) "Political subdivision" has the same meaning as in section 2744.01 of the Revised Code.

(8) "Record" means any information that is stored in an electronic medium and is retrievable in perceivable form. "Record" does not include any publicly available directory containing information an individual voluntarily has consented to have publicly disseminated or listed, such as name, address, or telephone number.

(9) "Redacted" means altered or truncated so that no more than the last four digits of a social security number, driver's license number, state identification card number, account number, or credit or debit card number is accessible as part of the data.

(10) "State agency" has the same meaning as in section 1.60 of the Revised Code, except that "state agency" does not include an agency that is a covered entity as defined in 45 C.F.R. 160.103, as amended.

(11) "System" means, notwithstanding section 1347.01 of the Revised Code, any collection or group of related records that are kept in an organized manner, that are maintained by a state agency or an agency of a political subdivision, and from which personal information is retrieved by the name of the individual or by some identifying number, symbol, or other identifier assigned to the individual. "System" does not include any collected archival records in the custody of or administered under the authority of the Ohio historical society, any published directory, any reference material or newsletter, or any routine information that is maintained for the purpose of internal office administration of the agency, if the use of the directory, material, newsletter, or information would not adversely affect an individual and if there has been no unauthorized external breach of the directory, material, newsletter, or information.

(B)(1) Any state agency or agency of a political subdivision that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system, following its discovery or notification of the breach of the security of the system, to any resident of this state whose personal information was, or reasonably is believed to have been, accessed and acquired by an unauthorized person if the access and acquisition by the unauthorized person causes or reasonably is believed will cause a material risk of identity theft or other fraud to the resident. The disclosure described in this division may be made pursuant to any provision of a contract entered into by the state agency or agency of a political subdivision with any person or another state agency or agency of a political subdivision prior to the date the breach of the security of the system occurred if that contract does not conflict with any provision of this section. For purposes of this section, a resident of this state is an individual whose principal mailing address as reflected in the records of the state agency or agency of a political subdivision is in this state.

(2) The state agency or agency of a political subdivision shall make the disclosure described in division (B)(1) of this section in the most expedient time possible but not later than forty-five days following its discovery or notification of the breach in the security of the system, subject to the legitimate needs of law enforcement activities described in division (D) of this section and consistent with any measures necessary to determine the scope of the breach, including which residents' personal information was accessed and acquired, and to restore the reasonable integrity of the data system.

(C) Any state agency or agency of a political subdivision that, on behalf of or at the direction of another state agency or agency of a political subdivision, is the custodian of or stores computerized data that includes personal information shall notify that other state agency or agency of a political subdivision of any breach of the security of the system in an expeditious manner, if the personal information was, or reasonably is believed to have been, accessed and acquired by an unauthorized person and if the access and acquisition

by the unauthorized person causes or reasonably is believed will cause a material risk of identity theft or other fraud to a resident of this state.

(D) The state agency or agency of a political subdivision may delay the disclosure or notification required by division (B), (C), or (F) of this section if a law enforcement agency determines that the disclosure or notification will impede a criminal investigation or jeopardize homeland or national security, in which case, the state agency or agency of a political subdivision shall make the disclosure or notification after the law enforcement agency determines that disclosure or notification will not compromise the investigation or jeopardize homeland or national security.

(E) For purposes of this section, a state agency or agency of a political subdivision may disclose or make a notification by any of the following methods:

(1) Written notice;

(2) Electronic notice, if the state agency's or agency of a political subdivision's primary method of communication with the resident to whom the disclosure must be made is by electronic means;

(3) Telephone notice;

(4) Substitute notice in accordance with this division, if the state agency or agency of a political subdivision required to disclose demonstrates that the agency does not have sufficient contact information to provide notice in a manner described in division (E)(1), (2), or (3) of this section, or that the cost of providing disclosure or notice to residents to whom disclosure or notification is required would exceed two hundred fifty thousand dollars, or that the affected class of subject residents to whom disclosure or notification is required exceeds five hundred thousand persons. Substitute notice under this division shall consist of all of the following:

(a) Electronic mail notice if the state agency or agency of a political subdivision has an electronic mail address for the resident to whom the disclosure must be made;

(b) Conspicuous posting of the disclosure or notice on the state agency's or agency of a political subdivision's web site, if the agency maintains one;

(c) Notification to major media outlets, to the extent that the cumulative total of the readership, viewing audience, or listening audience of all of the outlets so notified equals or exceeds seventy-five per cent of the population of this state.

(5) Substitute notice in accordance with this division, if the state agency or agency of a political subdivision required to disclose demonstrates that the agency has ten employees or fewer and that the cost of providing the disclosures or notices to residents to whom disclosure or notification is required will exceed ten thousand dollars. Substitute notice under this division shall consist of all of the following:

(a) Notification by a paid advertisement in a local newspaper that is distributed in the geographic area in which the state agency or agency of a political subdivision is located, which advertisement shall be of sufficient size that it covers at least one-quarter of a page in the newspaper and shall be published in the newspaper at least once a week for three consecutive weeks;

(b) Conspicuous posting of the disclosure or notice on the state agency's or agency of a political subdivision's web site, if the agency maintains one;

(c) Notification to major media outlets in the geographic area in which the state agency or agency of a political subdivision is located.

(F) If a state agency or agency of a political subdivision discovers circumstances that require disclosure under this section to more than one thousand residents of this state involved in a single occurrence of a breach of the security of the system, the state agency or agency of a political subdivision shall notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis of the timing, distribution, and content of the disclosure given by the state agency or agency of a political subdivision to the residents of this state. In no case shall a state agency or agency of a political subdivision that is required to make a notification required by this division delay any disclosure or notification required by division (B) or (C) of this section in order to make the notification required by this division.

(G) The attorney general, pursuant to sections 1349.191 and 1349.192 of the Revised Code, may conduct an investigation and bring a civil action upon an alleged failure by a state agency or agency of a political subdivision to comply with the requirements of this section.

ORC 1347.15 Access rules for confidential personal information.

(A) As used in this section:

(1) "Confidential personal information" means personal information that is not a public record for purposes of section 149.43 of the Revised Code.

(2) "State agency" does not include the courts or any judicial agency, any state-assisted institution of higher education, or any local agency.

(B) Each state agency shall adopt rules under Chapter 119. of the Revised Code regulating access to the confidential personal information the agency keeps, whether electronically or on paper. The rules shall include all the following:

(1) 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;

(2) 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 confidential personal information;

(3) References to the applicable federal or state statutes or administrative rules that make the confidential personal information confidential;

(4) A procedure that requires the state agency to do all of the following:

(a) Provide that any upgrades to an existing computer system, or the acquisition of any new computer system, that stores, manages, or contains confidential personal information include a mechanism for recording specific access by employees of the state agency to confidential personal information;

(b) Until an upgrade or new acquisition of the type described in division (B)(4)(a) of this section occurs, except as otherwise provided in division (C)(1) of this section, keep a log that records specific access by employees of the state agency to confidential personal information;

(5) A procedure that requires the state agency to comply with a written request from an individual for a list of confidential personal information about the individual that the state agency keeps, unless the confidential personal information relates to an investigation about the individual based upon specific statutory authority by the state agency;

(6) A procedure that requires the state agency to notify each person whose confidential personal information has been accessed for an invalid reason by employees of the state agency of that specific access;

(7) A requirement that the director of the state agency designate an employee of the state agency to serve as the data privacy point of contact within the state agency to work with the chief privacy officer within the office of information technology to ensure that confidential personal information is properly protected and that the state agency complies with this section and rules adopted thereunder;

(8) A requirement that the data privacy point of contact for the state agency complete a privacy impact assessment form; and

(9) A requirement that a password or other authentication measure be used to access confidential personal information that is kept electronically.

(C)(1) A procedure adopted pursuant to division (B)(4) of this section shall not require a state agency to record in the log it keeps under division (B)(4)(b) of this section any specific access by any employee of the agency to confidential personal information in any of the following circumstances:

(a) The access occurs as a result of research performed for official agency purposes, routine office procedures, or incidental contact with the information, unless the conduct resulting in the access is

specifically directed toward a specifically named individual or a group of specifially named individuals.

(b) The access is to confidential personal information about an individual, and the access occurs as a result of a request by that individual for confidential personal information about that individual.

(2) Each state agency shall establish a training program for all employees of the state agency described in division (B)(1) of this section so that these employees are made aware of all applicable statutes, rules, and policies governing their access to confidential personal information.

The office of information technology shall develop the privacy impact assessment form and post the form on its internet web site by the first day of December each year. The form shall assist each state agency in complying with the rules it adopted under this section, in assessing the risks and effects of collecting, maintaining, and disseminating confidential personal information, and in adopting privacy protection processes designed to mitigate potential risks to privacy.

(D) Each state agency shall distribute the policies included in the rules adopted under division (B) of this section to each employee of the agency described in division (B)(1) of this section and shall require that the employee acknowledge receipt of the copy of the policies. The state agency shall create a poster that describes these policies and post it in a conspicuous place in the main office of the state agency and in all locations where the state agency has branch offices. The state agency shall post the policies on the internet web site of the agency if it maintains such an internet web site. A state agency that has established a manual or handbook of its general policies and procedures shall include these policies in the manual or handbook.

(E) No collective bargaining agreement entered into under Chapter 4117. of the Revised Code on or after the effective date of this section shall prohibit disciplinary action against or termination of an employee of a state agency who is found to have accessed, disclosed, or used personal confidential information in violation of a rule adopted under division (B) of this section or as otherwise prohibited by law.

(F) The auditor of state shall obtain evidence that state agencies adopted the required procedures and policies in a rule under division (B) of this section, shall obtain evidence supporting whether the state agency is complying with those policies and procedures, and may include citations or recommendations relating to this section in any audit report issued under section 117.11 of the Revised Code.

(G) A person who is harmed by a violation of a rule of a state agency described in division (B) of this section may bring an action in the court of claims, as described in division (F) of section 2743.02 of the Revised Code, against any person who directly and proximately caused the harm.

(H)(1) No person shall knowingly access confidential personal information in violation of a rule of a state agency described in division (B) of this section.

(2) No person shall knowingly use or disclose confidential personal information in a manner prohibited by law.

(3) No state agency shall employ a person who has been convicted of or pleaded guilty to a violation of division (H)(1) or (2) of this section.

(4) A violation of division (H)(1) or (2) of this section is a violation of a state statute for purposes of division (A) of section 124.341 of the Revised Code.

ORC 1347.99 Penalty.

(A) No public official, public employee, or other person who maintains, or is employed by a person who maintains, a personal information system for a state or local agency shall purposely refuse to comply with division (E), (F), (G), or (H) of section 1347.05, section 1347.071, division (A), (B), or (C) of section 1347.08, or division (A) or (C) of section 1347.09 of the Revised Code. Whoever violates this section is guilty of a minor misdemeanor.

(B) Whoever violates division (H)(1) or (2) of section 1347.15 of the Revised Code is guilty of a misdemeanor of the first degree.

Fair Information Practice Principles (FIPPS)

Transparency: The organization should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of personally identifiable information (PII).

Individual Participation: The organization should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of PII. The organization should also provide mechanisms for appropriate access, correction, and redress regarding the organization's use of PII.

Purpose Specification: The organization should specifically articulate the authority that permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.

Data Minimization: The organization should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s).

Use Limitation: The organization should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected.

Data Quality and Integrity: The organization should, to the extent practicable, ensure that PII is accurate, relevant, timely, and complete.

Security: The organization should protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

Accountability and Auditing: The organization should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

Office of Information Security and Privacy| 30 E. Broad Street,
40th Floor |Columbus, Ohio 43215
614.644.9391|Privacy.Ohio.gov
Robert Blair, Director

Office of Information Security and Privacy
Ohio Revised Code 1347.15 Guidance

Privacy Impact Assessments

Ohio Privacy Impact Statements and Assessment 2012
Privacy Threshold Assessment Template
Privacy Impact Assessment Template

Templates for ORC 1347.15 Policies and Procedures

Ohio Privacy Policies Framework
Template Policy on Protecting Privacy
Procedure Template - Accessing and Logging CPI (Computer)
Procedure Template - Incident Response for Invalid Access of Confidential or Sensitive PII
Procedure Template - Accessing CPI (Paper)
Procedure Template - Requests for PI
Procedure Template - Accessing Sensitive Data

Guidance

Ohio Revised Code Section 1347.15
Ohio Revised Code Chapter 1347: Personal Information Systems

Guide to Implementing Section 1347.15 of the Ohio Revised Code (Under Revision)
Interim Policy on Logging Access to Confidential Personal Information (State of Ohio)

Access Policies Resource Kit (State of Ohio)
Role and Identity Management Resource Kit (State of Ohio)
Ohio Revised Code Chapter 1347: Personal Information Systems
Preliminary Checklist for Applying "Confidential Personal Information" to Priority Systems
Data Classification Resource Kit (State of Ohio)

Contact Information

30 East Broad St., 40th Floor
Columbus, Ohio 43215
614-644-9391
www.privacy.ohio.gov

Daren Arnold, State Chief Privacy Officer
614-752-7204
daren.arnold@oit.ohio.gov

David Shaw, State Chief Information Security Officer
614-644-9389
david.shaw@das.ohio.gov

Kevin Brown, Privacy Architect Consultant
614-387-5682
kevin.brown@oit.ohio.gov

Jillian Burner, Administrative Professional
614-387-0320
Jillian.burner@oit.ohio.gov