



Privacy Policy Implementation Resources

Office of Privacy and Data Protection, August 2024

Today's Agenda

- **Introduction**
- **Example Privacy Policy**
Sofiya Ahmed (WaTech)
- **Privacy Notice Implementation Guidance**
Matt King (WaTech) and Sam Méndez (HCA)
- **Policy Crosswalk**
Katy Ruckle (WaTech)



What's in it?

- 14 sections
- Reinforces existing legal requirements and existing practices
- Many sections are supported by existing OPDP resources
- Includes functional needs (not technical)
- Effective June 24, 2024

Policy Requirements



Section	
1	Statement of agency responsibility
2	Annual privacy assessment
3	Privacy contacts
4	Data discovery and documentation
5	Policies and procedures
6	Privacy impact assessments
7	Training and awareness

Section	
8	Data sharing agreements
9	Data disposal
10	Privacy notices
11	Individual participation
12	Incident response
13	Monitoring and periodic review
14	Biometrics

Section 5 – Policies and procedures

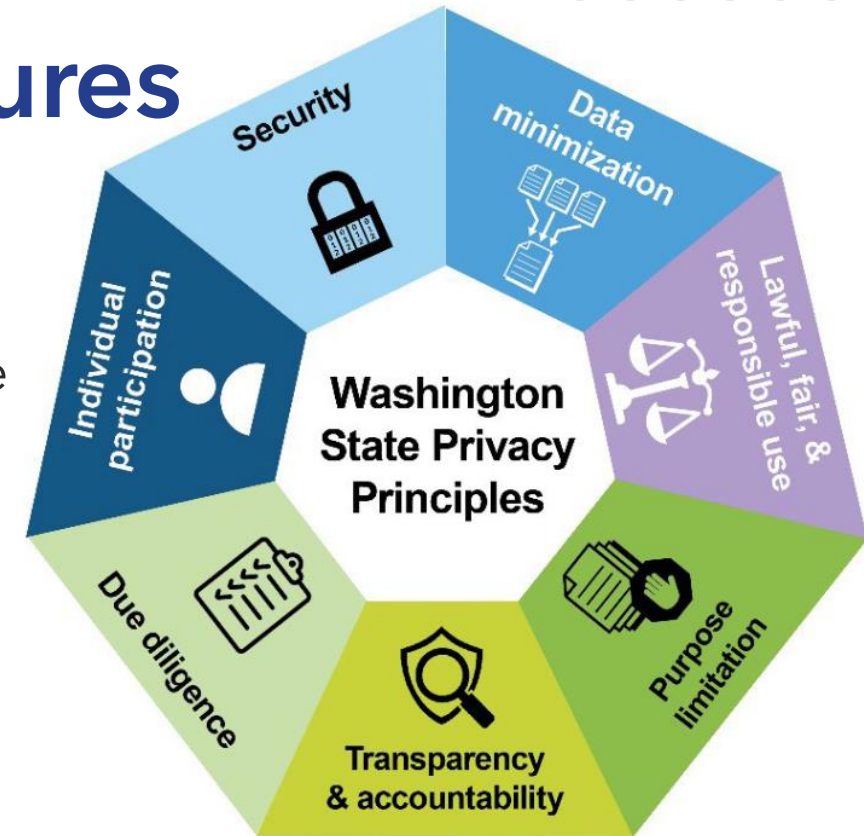
Highlights

- “Agencies that process personal information must establish policies and procedures consistent with the Washington State Agency Privacy Principles and other applicable laws or handling standards.”

- Policies must ensure that privacy is integrated into activities and projects with personal information

Resources

- [Washington State Agency Privacy Principles](#)
- [Washington State Agency Privacy Principles and Risk Management](#) (webinar)
- [Incorporating Privacy into the System Development Process](#) (webinar)





Section 10 – Privacy notices

Highlights

- “Agencies must be transparent about how they process personal information by publishing privacy notices”
- Notices should provide meaningful, understandable information
- Routinely review and update as necessary to match current practices

Resources

[Privacy Notices](#) (webinar)



Example Privacy Policy

Example Privacy Policy



Replaces:
NEW

WaTech
Washington Technology Solutions
WaTech Privacy Policy

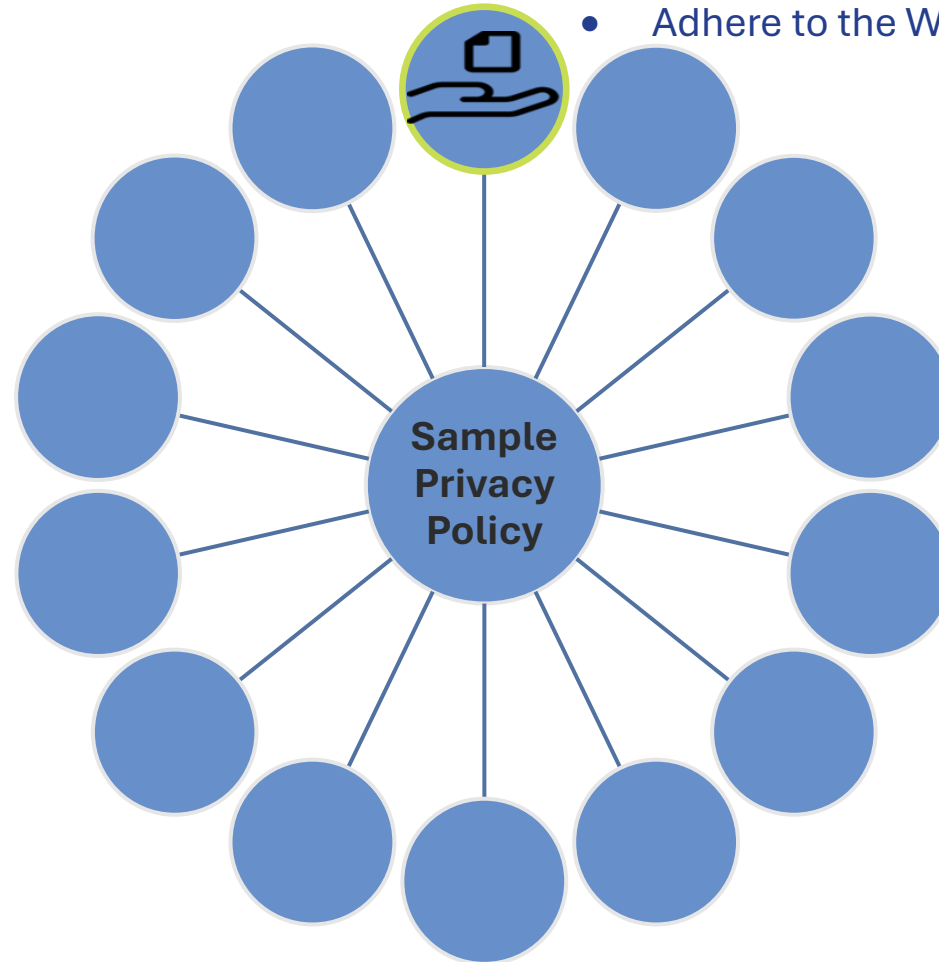
See Also:
[RCW 42.105.369](#) Office of privacy and data protection

- 1. WaTech must protect personal information it processes to provide services, perform government functions, and handle information responsibly. To maintain public trust, safeguard sensitive information and comply with regulations WaTech must adhere to the established privacy principles articulated by the Office of Privacy and Data Protection. See [RCW 43.105.369\(3\)\(c\)](#).**
- 2. WaTech must complete the privacy assessment survey required under the annual certification process. See [Technology Policies, Standards, and Procedures \(7.b\)](#).**
 - a. The WaTech Privacy Officer must complete the annual privacy assessment survey.
 - b. As part of the annual privacy assessment survey process, the WaTech Privacy Officer must review and inventory the personally identifiable information (PII) it processes and the correlating privacy practices.
 - c. The WaTech Privacy Officer will consult and collaborate with other WaTech teams as needed to complete the annual privacy assessment survey.
- 3. WaTech designates the WaTech Privacy Officer as its privacy contact.**
 - a. The WaTech Privacy Officer is the official contact for privacy matters specific to WaTech agency business.
 - b. The State Chief Privacy Officer is the contact for privacy matters that have external or state-wide impacts.
- 4. WaTech must understand the personal information it processes. This work will be completed by the WaTech Privacy Officer in coordination with other relevant WaTech Teams including but not limited to the Office of Cybersecurity, Strategy and Management, Architecture and Innovation, and the Records Management Unit.**
 - a. WaTech will classify data into categories based on its sensitivity and handling requirements.
 - b. WaTech will complete the application inventory as required by [MGMT-01](#)

- Also has 14 sections
- This example policy is modeled on WaTech's privacy policy
- Intended to serve as a resource

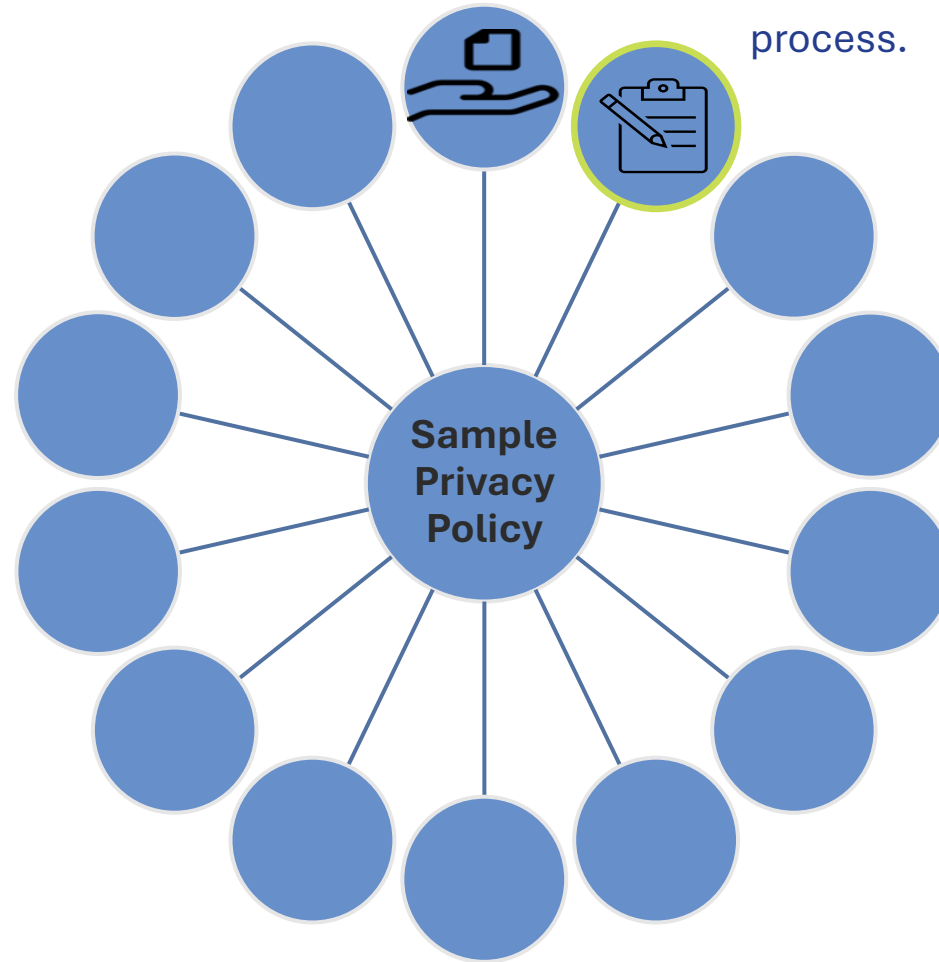
Section 1: Statement of agency responsibility

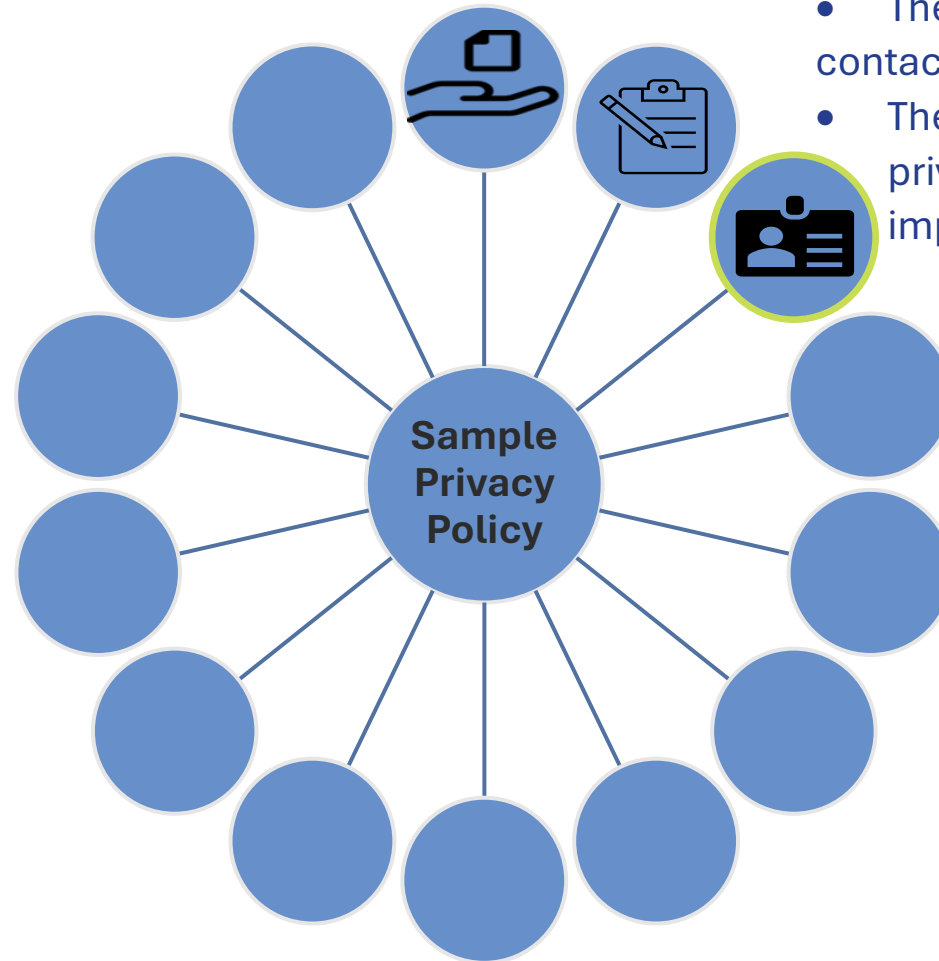
- Maintain public trust.
- Safeguard sensitive information.
- Comply with regulations.
- Adhere to the Washington State Privacy Principles.



Section 2: Annual privacy assessment

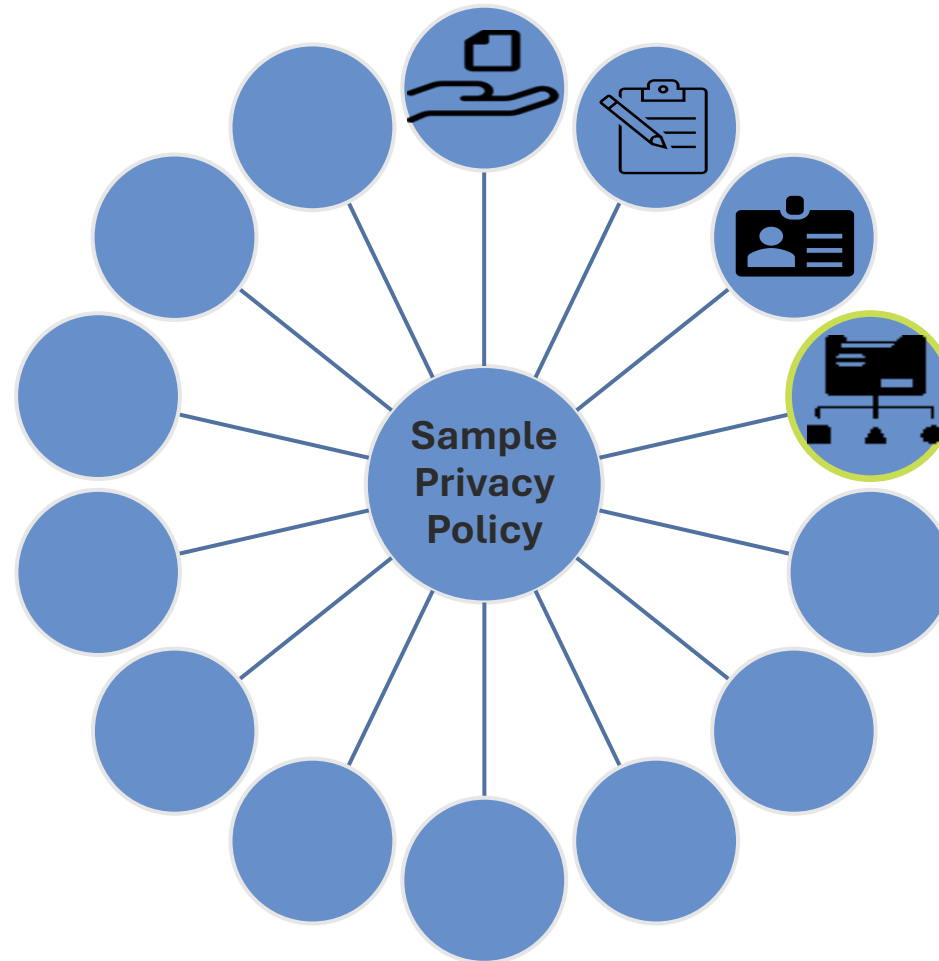
- Complete the annual privacy assessment survey.
- Review & Inventory of what personal information we process.





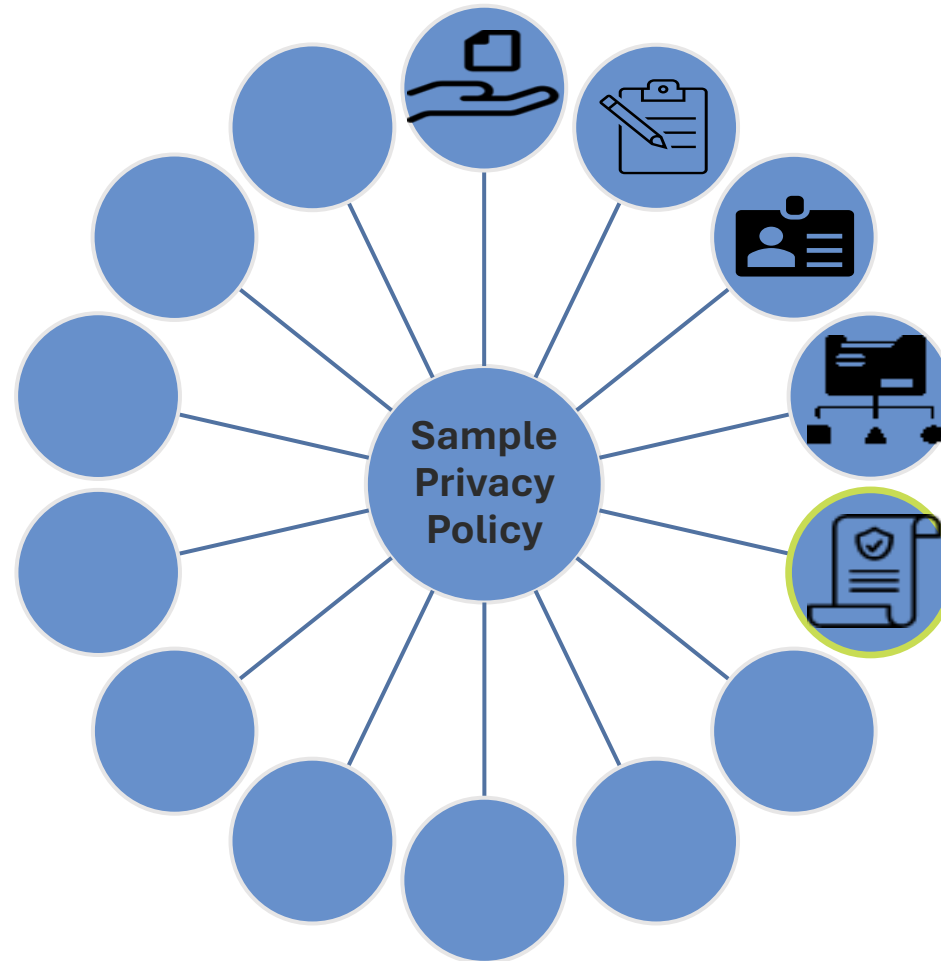
Section 3: Privacy contacts

- Designate privacy officer
- The WaTech Privacy Officer is the contact for privacy matters specific to our agency.
- The State Chief Privacy Officer is the contact of privacy matters that have external or state-wide impacts



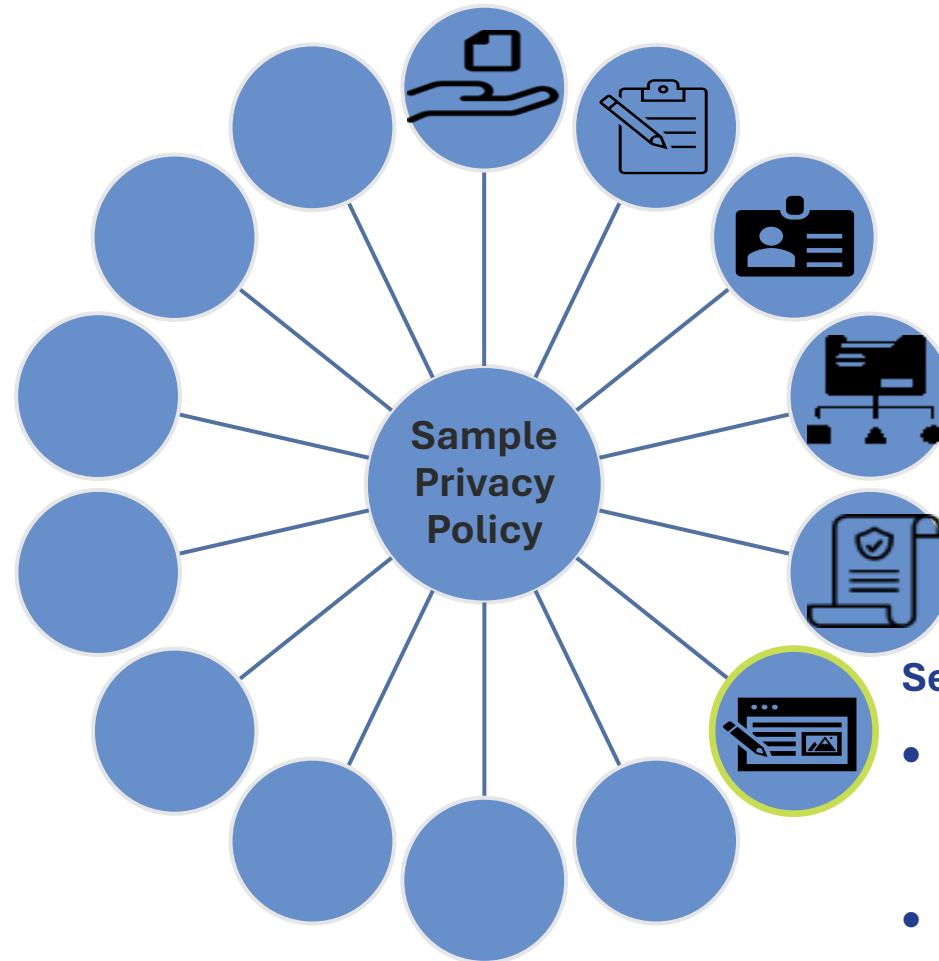
Section 4: Data discovery and documentation

- Classify data into categories based on sensitivity and handling requirements.
- Complete application inventory
- Maintain an up-to-date data inventory.



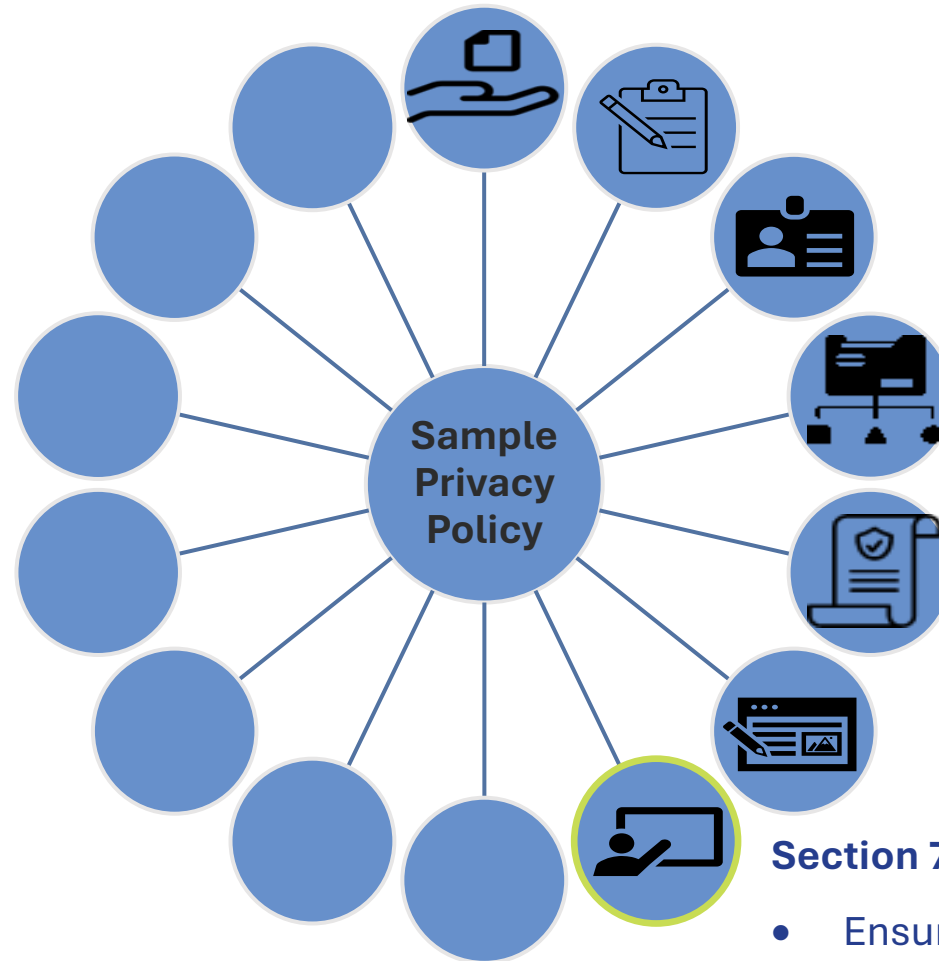
Section 5: Policies and procedures

- Integrate the WSAPP into projects involving personal information.
- Review projects involving personal information.
- Review all Terms of Services for services that involve personal information.



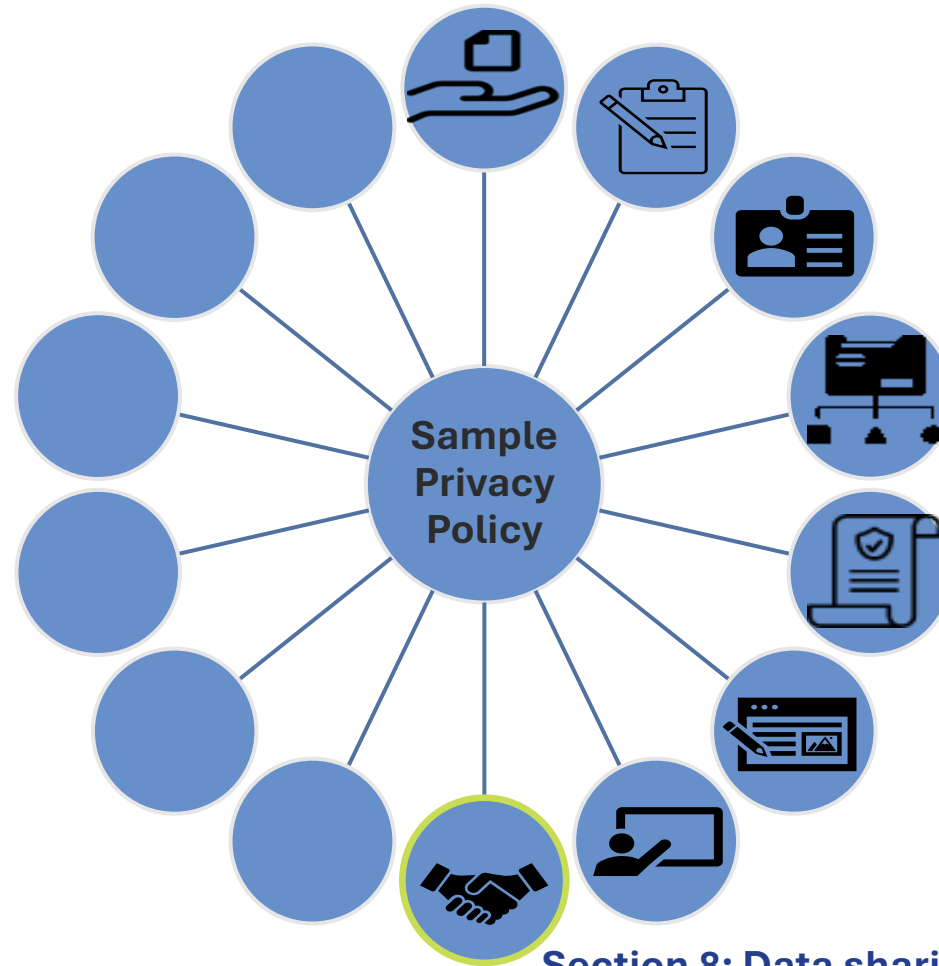
Section 6: Privacy impact assessments

- Complete privacy threshold analysis (PTA) & privacy impact assessments (PIA).
- Complete new PTAs within 10 days.



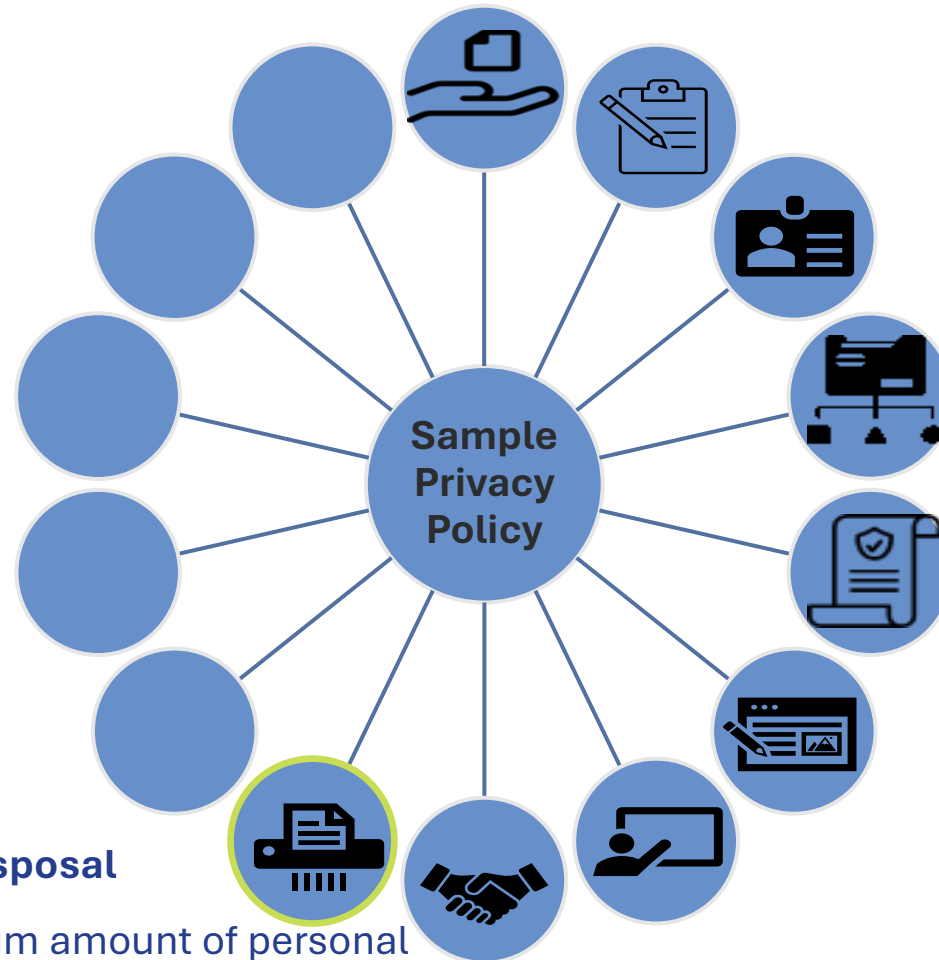
Section 7: Training and awareness

- Ensure all employees complete privacy training.
- Promote privacy awareness.



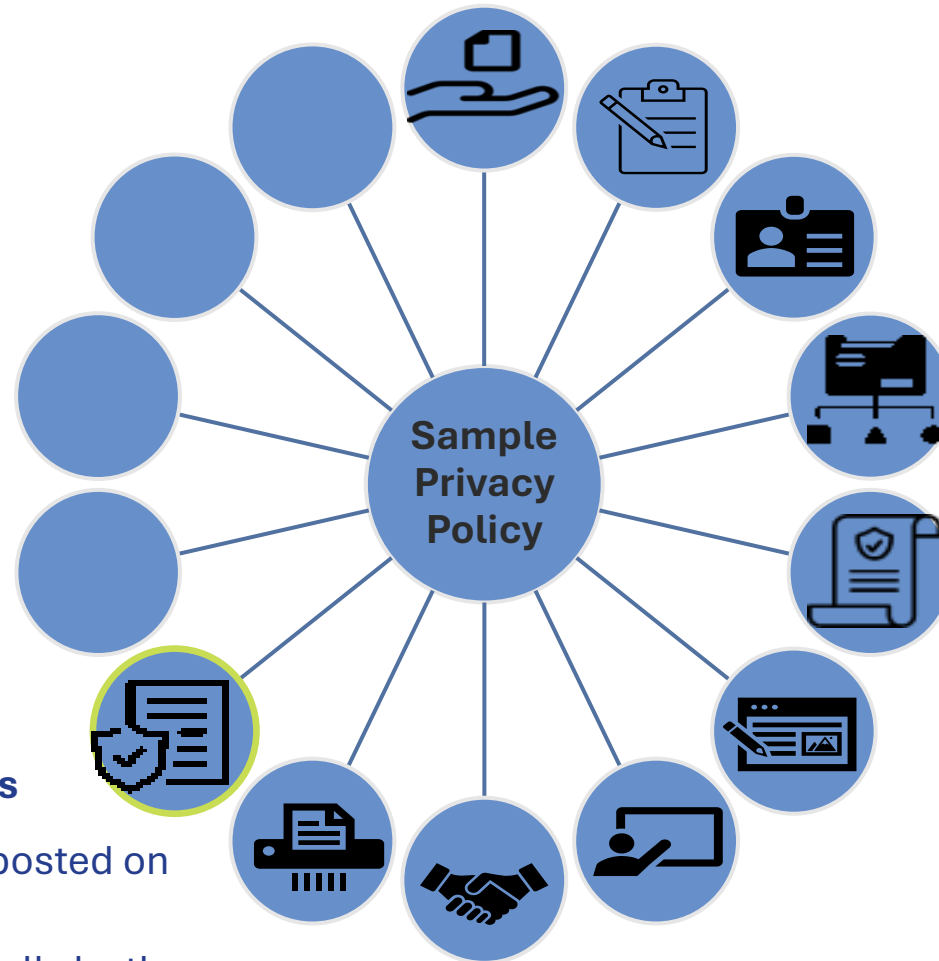
Section 8: Data sharing agreements

- Notify OPDP prior to the sale of personal information.
- Ensure Primary Service Agreement & Terms of Service comply with our DSA policy.



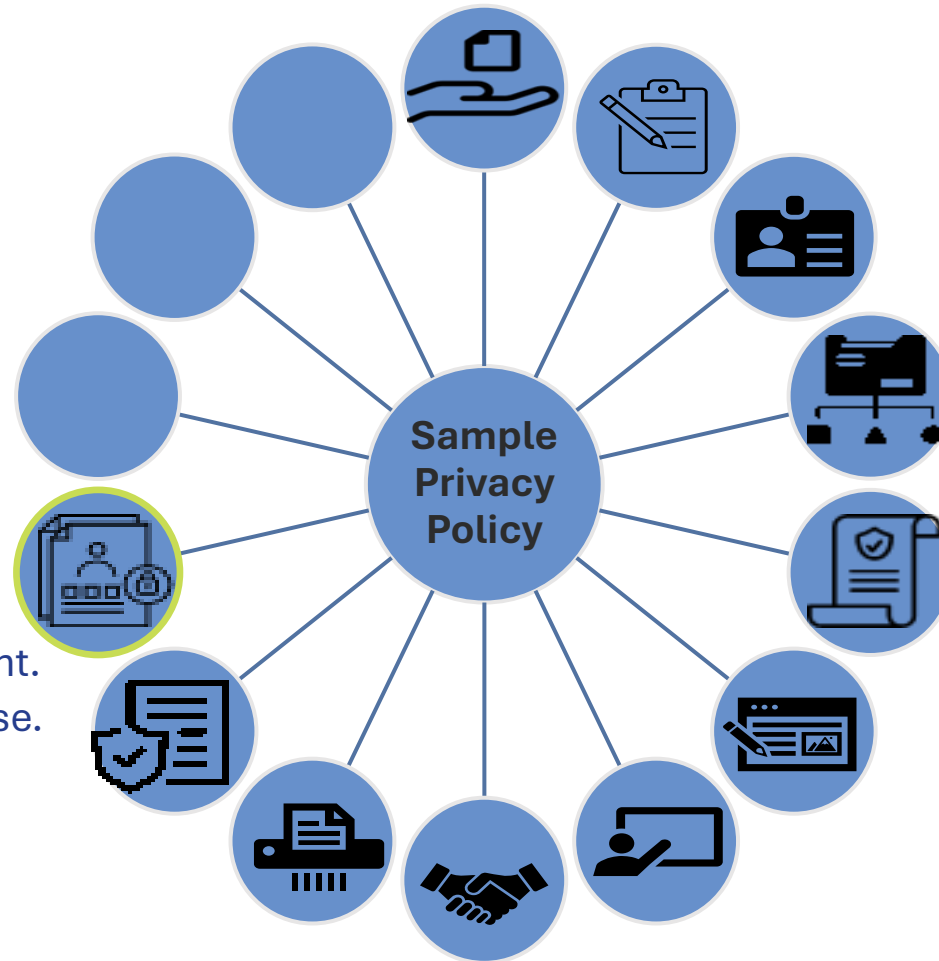
Section 9: Data disposal

- Collect minimum amount of personal information needed to accomplish a specific purpose.
- Collect & use personal information with appropriate legal authority.



Section 10: Privacy notices

- Privacy notices will be posted on our website.
- It will be reviewed annually by the privacy officer.

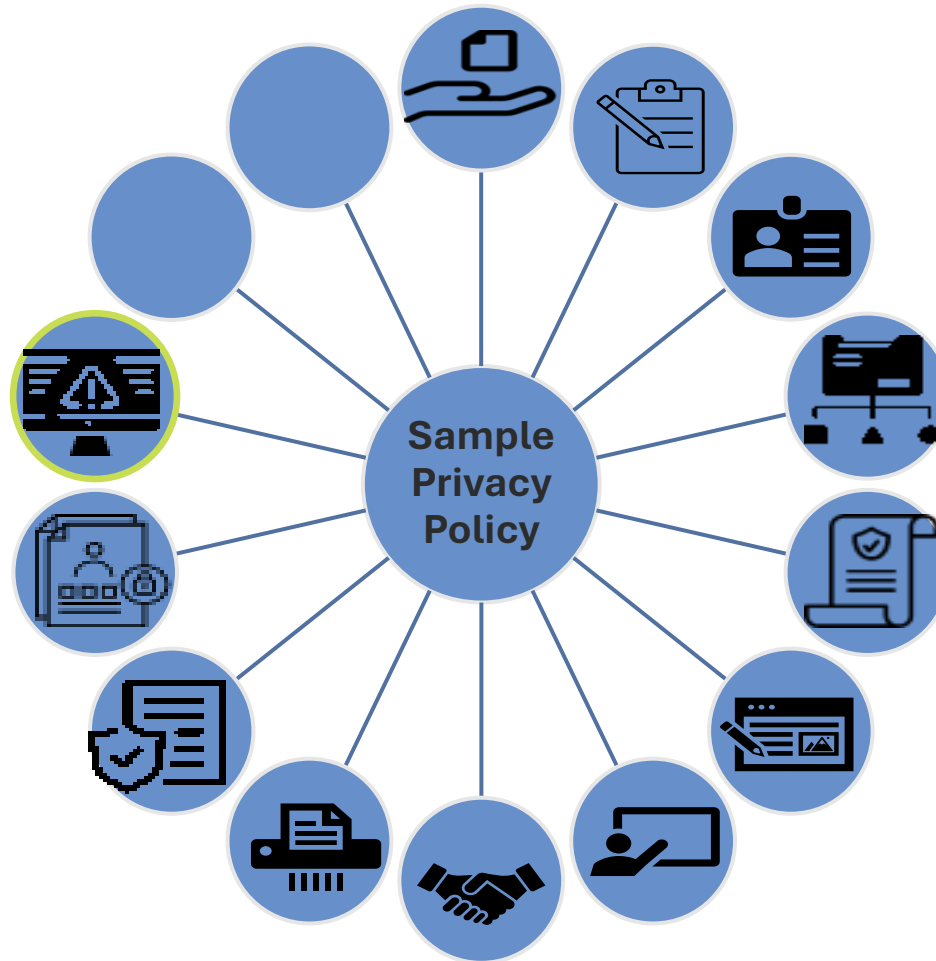


Section 11: Individual participation

- Provide, revoke, or manage consent.
- Opt-Out or restrict collection or use.
- Request corrections to inaccurate information.

Section 12: Incident response

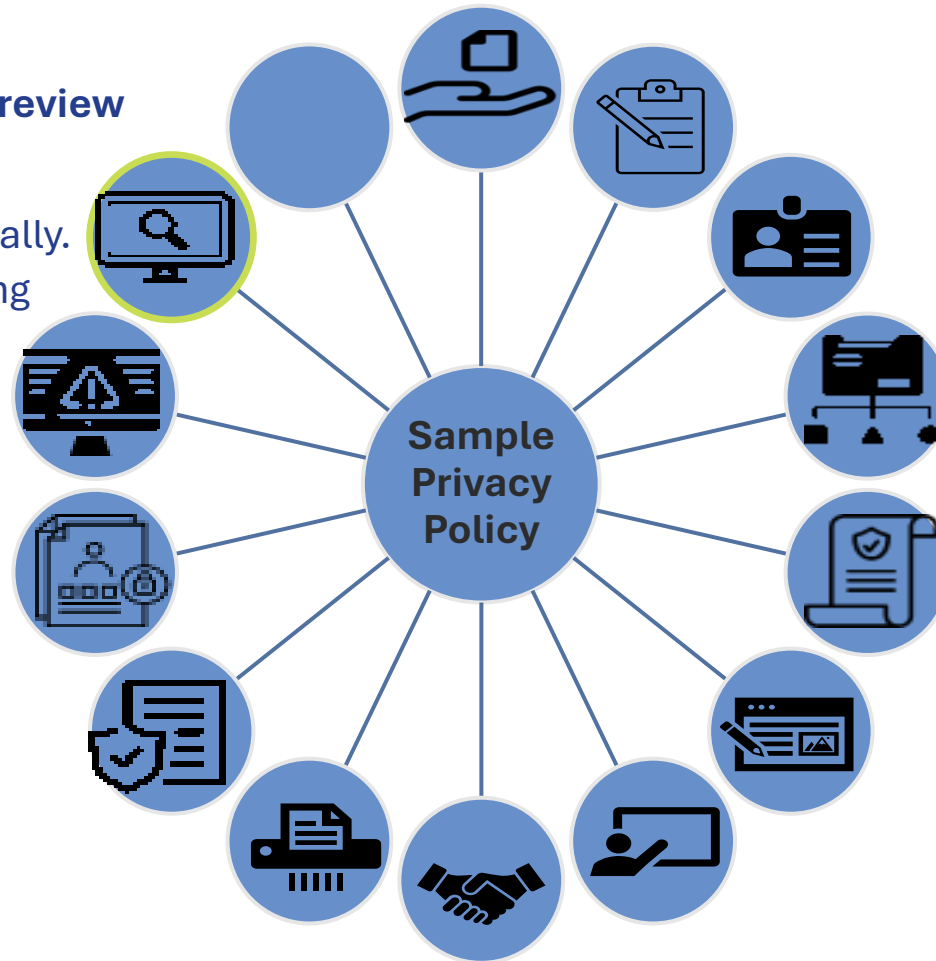
- Breach policy
- Incident Response Plan
- Data breach assessment form to determine if an incident requires notification.





Section 13: Monitoring and periodic review

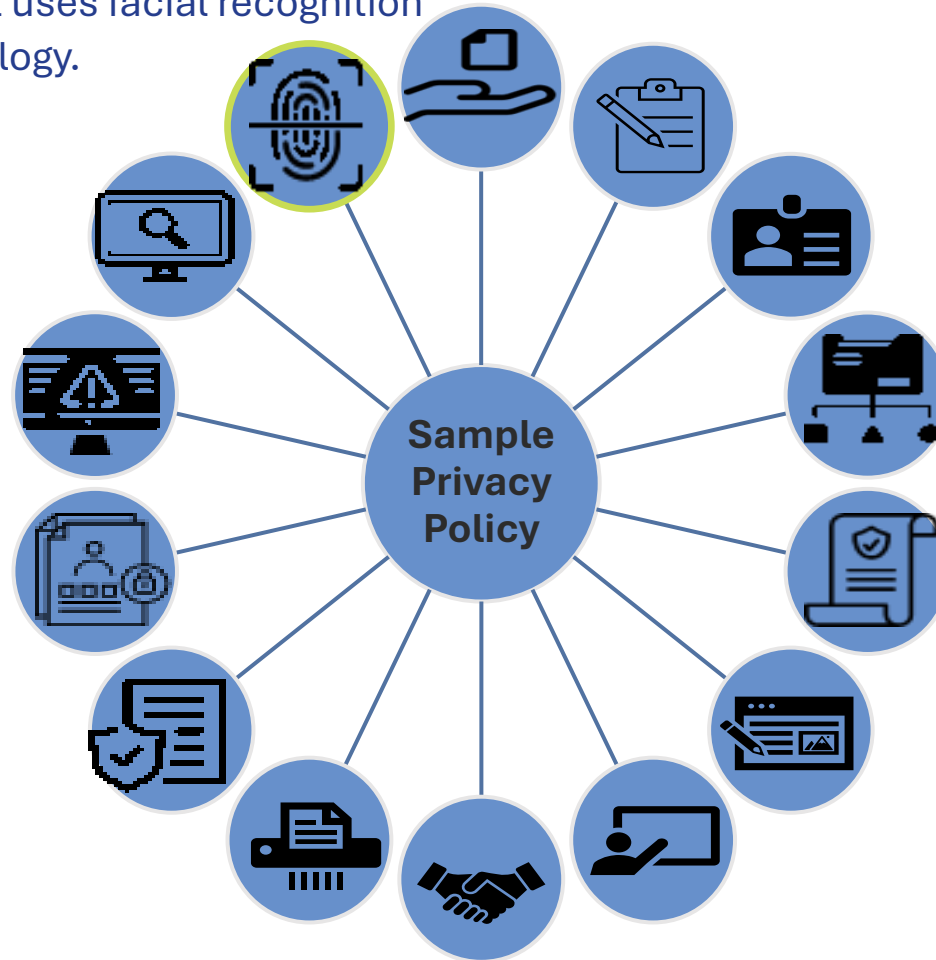
- Monitoring compliance with DSA.
- Reviewing the privacy notice annually.
- Measuring compliance with training requirements.



Section 14: Biometrics



- Our agency will adhere to facial recognition & biometric identifier laws when it uses facial recognition technology.





- [Privacy and Data Protection Policy](#)
- [Privacy and Data Protection Policy Webinar](#)
 - [Webinar Slide Deck](#)
- [Example Privacy Policy](#)



Privacy Notice Implementation Guidance

Guidance Overview



	Privacy Notice	Website Privacy Notice	Privacy Policy
Aliases	Privacy Statement, Privacy Policy, Notice of Privacy Practices	Cookie Notice, Security Notice, Privacy Notice, Privacy Statement, Privacy Policy	
Associated principle	Transparency	Transparency	Accountability
Audience	External	External	Internal



- Agencies manage different types of personal information, collect it in different ways, use and share for different purposes, are subject to different laws, and have different missions
- Privacy notices must vary, too

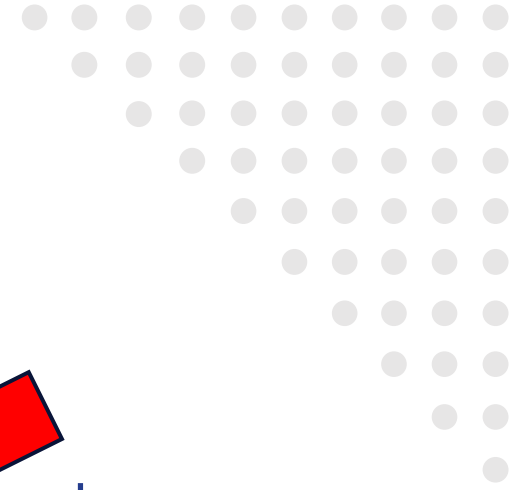


- Starting place for new notice, or tool to help review existing notices
- Some agencies subject to additional requirements
- 2 sections:
 - Implementation Considerations
 - Privacy Notice Content



Implementation Considerations

Plain language



~~This Privacy Policy is hereby provided pursuant to an accordance with applicable state law and regulatory provisions governing Personal Data processing. By accessing and utilizing, otherwise interacting with our services you expressly consent to the processing of Personal Data as defined under applicable law including but not limited to any and all identifiers and any other data elements pertaining to you, which may be processed by us, our affiliates, or our third-party processors~~



- Keep concise, avoid legalese
- If not possible to remove all terms of art -> provide clear definitions
- Provide translations
- [Plain language guidelines](#)

Accuracy and currency



- Inaccurate notice ≠ transparency
- Collaborate across disciplines to understand intended purposes and protection commitments
- Verify practices are actually in place

- Outdated notices ≠ accurate
- Change happens
 - Regulatory changes
 - Program changes
 - Technology changes
- Must be routinely reviewed and updated (*Data-03, section 10*)
- Recommendation = review annually, or any time there are known material changes

Method of Delivery



Linked on website footer	Posted in physical location for viewing
Linked on web form when people submit personal information	Mailed to physical address
E-mailed	Just-in-time electronic notice at point of information collection
Handed to someone in person	



- Consider:
 - Using more than one method
 - How your agency normally interacts with customers
 - Whether to gather acknowledgement
- At a minimum, must be posted on each agency's website (*Data-03, section 10*)
- Some privacy laws have specific delivery method requirements



- Initial privacy notice – Provide during initial interaction.
- Periodic privacy notice – Provide routine periodic updates when your agency has an ongoing relationship with customers.
- Revised privacy notice – Provide when there are material changes to privacy practices.
- Some privacy laws have specific timing requirements



- In addition to long form notice, consider other ways to effectively communicate information
 - Layered notices – Short explanations with most important information, additional layers provide more details
 - Dashboards – Interactive tools that explain practices and allow customers to manage preferences
 - Just-in-time notices – Link to notice right before information submitted, or a pop-up explaining why a specific data element is needed



Privacy Notice Content



- The [Privacy and Data Protection Policy, Data-03](#), requires privacy notices to include at least:
 - The types of personal information the agency processes
 - How and why the agency processes personal information
 - Who the agency shares personal information with, if applicable
 - How individuals can exercise any applicable rights to access or control their personal information
 - How to contact the agency

The types of personal information the agency processes

- Provide enough detail to be meaningful, but specific data elements not required
- Examples of categories include:
 - Demographic information
 - Biometric information
 - Communications
 - Location information
 - Website usage
- Also explain how anonymous or aggregate information is used

How and why the agency processes personal information

- Overall purpose – Agency purpose, including the functions it performs or services or benefits it provides
- Type of data – Types of personal information, and anonymous or aggregated information
- Specific uses – Make the connection between **what** information is collected and **why**
- Methods of collection – Make the connection between **what** information is collected and **how**
- Who data is shared with – Describe **what** information is shared with **whom** and **why**
- Retention and deletion – How long do you commit to retain information, and when will you delete it
- Data security – General statement of security practices

Who the agency shares information with, if applicable

- Who information is shared with – Describe the types of third parties you send personal information to
- Why it is shared – For each category of recipient, describe the purpose
- How it is protected once shared – Describe whether the information is still subject to the same level of protections once shared
- Specifically address data sales, if applicable

How individuals can exercise any applicable rights to access or control their information

- Examples include:
 - Confirming whether the agency processes personal information
 - Accessing or correcting information
 - Asking for information to be deleted
 - Opting in or out of specific uses or disclosures
 - Withdrawing prior consent
- Describe which types of participation are available and how to exercise that control
- At a minimum, include how a person can access their information

How to contact the agency



- Clearly identify how to get additional information, ask questions or make complaints
- At a minimum, should include contact information for appropriate agency contacts
 - May include other information like resource links or regulator contact information

How HCA does Notices of Privacy Practices (NPP)

Sam Mendez, Privacy Officer

HIPAA

[45 CFR 164.520](#)

⦿ § 164.520 Notice of privacy practices for protected health information.

(a) *Standard: Notice of privacy practices* –

(1) *Right to notice.* Except as provided by paragraph (a)(3) or (4) of this section, **an individual has a right to adequate notice of the uses and disclosures of protected health information that may be made by the covered entity, and of the individual's rights and the covered entity's legal duties with respect to protected health information.**

(2) *Notice requirements for covered entities creating or maintaining records subject to 42 U.S.C. 290dd-2.* As provided in [42 CFR 2.22](#), an individual who is the subject of records protected under [42 CFR part 2](#) has a right to adequate notice of the uses and disclosures of such records, and of the individual's rights and the covered entity's legal duties with respect to such records.

(3) *Exception for group health plans.*

(i) An individual enrolled in a group health plan has a right to notice:

(A) From the group health plan, if, and to the extent that, such an individual does not receive health benefits under the group health plan through an insurance contract with a health insurance issuer or HMO; or

(B) From the health insurance issuer or HMO with respect to the group health plan

HIPAA

45 CFR 164.520

(b) *Implementation specifications: Content of notice* –

(1) **Required elements.** The covered entity, including any covered entity receiving or maintaining records subject to [42 U.S.C. 290dd-2](#), must provide a notice that is written in plain language and that contains the elements required by this paragraph.

(i) **Header.** The notice must contain the following statement as a header or otherwise prominently displayed:

“THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.”

(ii) **Uses and disclosures.** The notice must contain:

(A) A description, including at least one example, of the types of uses and disclosures that the covered entity is permitted by this subpart to make for each of the following purposes: treatment, payment, and health care operations.

(B) A description of each of the other purposes for which the covered entity is permitted or required by this subpart to use or disclose protected health information without the individual's written authorization.

(C) If a use or disclosure for any purpose described in [paragraphs \(b\)\(1\)\(ii\)\(A\) or \(B\)](#) of this section is prohibited or materially limited by other applicable law, such as [42 CFR part 2](#), the description of such use or disclosure must reflect the more

HCA Has Two NPPs

[HCA's NPP Homepage](#)

[Apple Health \(Medicaid\) NPP](#)

[UMP NPP](#)

Why have two notices?

HCA Has Two NPPs

- Each notice serves a different population
 - UMP NPP serves those in the Uniform Medical Plan (PEBB/SEBB)
 - Apple Health (Medicaid) NPP serves WA Medicaid recipients
- We could probably have a single notice and still be HIPAA compliant
- Uses & disclosures may differ depending on the program, so two NPPs allows HCA to be more nimble in how NPPs are updated
- A lot of both NPPs are identical (individual rights, HCA's obligations, etc.)

HCA Has Two NPPs

- These notices are worded differently (they were written at different times)
 - E.g. UMP NPP starts with an upfront explanation of how HCA can use/disclose PHI without patient's authorization
 - E.g. Apple Health NPP starts with the patient's rights
- There's a lot of discretion
- We might still revise how these NPPs are framed
- We still have to revise them based on revisions to HIPAA



Private sector examples

- [The Walt Disney Company](#)
- [Google](#)
- [Airbnb](#)
- [Pinterest](#)
- [Snapchat](#)

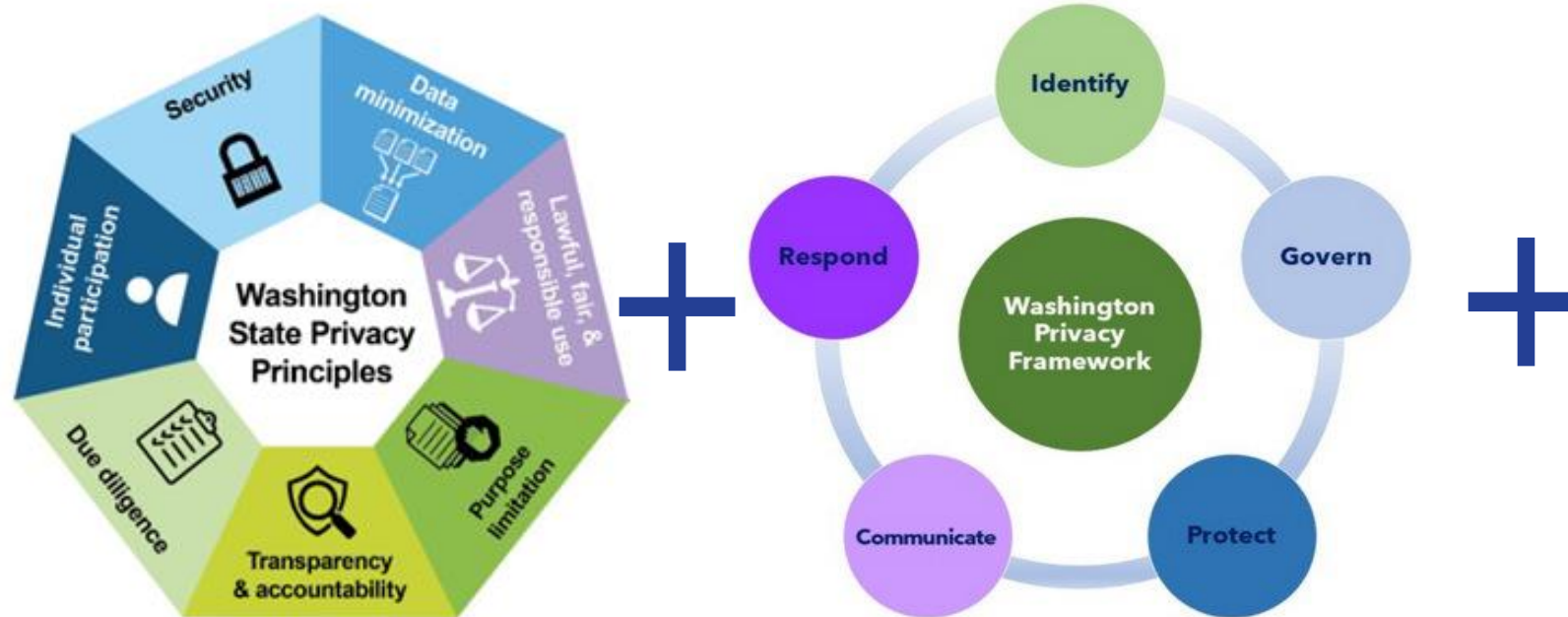
Regulatory examples:

- HIPAA Model Privacy Notice Template from U.S. Health and Human Services Office of Civil Rights: <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/model-notices-privacy-practices/index.html>
- FERPA Model Annual Notices from U.S. Department of Education: <https://studentprivacy.ed.gov/annual-notices>
- GLBA Model Privacy Form from U.S. Securities and Exchange Commission: https://www.sec.gov/rules/final/2009/34-61003_modelprivacyform.pdf



Policy Crosswalk

Policy Crosswalk



DATA-03
State CIO Adopted: June 24, 2024
TSB Approved: June 24, 2024
Sunset Review: June 24, 2027

WaTech
Washington Technology Solutions

PRIVACY AND DATA PROTECTION POLICY




Replaces:
NEW

See Also:
RCW 43.105.054 OCIO Governance
RCW 43.105.205 (3) Higher Ed
RCW 43.105.020 (23) "State agency"
RCW 42.105.369 Office of privacy and data protection
RCW 43.105.365 Accuracy, integrity, and privacy of records and information

1. State agencies have an obligation to protect the [personal information](#) they [process](#) to provide services and perform government functions and handle that information responsibly.
 - a. Effective privacy practices and responsible information processing enable success by reducing risk and building trust.
2. Agencies must complete the annual privacy assessment survey conducted by the Office of Privacy and Data Protection as part of the annual certification process. See [Technology Policies, Standards, and Procedures \(7.b.\)](#)
 - a. As part of the annual privacy assessment survey, agencies must indicate whether or not they process personal information.
3. Agencies must designate a privacy contact.
 - a. Designating a contact ensures accountability and efficient enterprise privacy communications.
 - b. The designated contact may or may not work full-time on privacy.
 - c. Resources dedicated to privacy will vary between agencies based on the size of the agency and the scope and scale of personal information the agency processes.
 - d. Privacy and data protection is multi-disciplinary. This means different positions and functions may implement or influence privacy practices. Specific privacy tasks will often be allocated across different functions of each agency. Examples of functions that may work on privacy include, but are not limited, to data management, public records, risk management, data governance, information technology security, legal, contracts and audit.

Policy Crosswalk



<p><u>Privacy and Data Protection Policy</u></p> 	<p><u>Privacy Framework for State Agencies</u></p> 	<p><u>Washington State Agency Privacy Principles</u></p> 
<p>Section 1: State agencies have an obligation to protect the <u>personal information</u> they process to provide services and perform government functions and handle that information responsibly.</p>	<p>Identify</p> <p>Govern</p> <p>Protect</p> <p>Communicate</p> <p>Respond</p>	<p>Lawful, Fair & Responsible Use; Data Minimization; Purpose Limitation; Transparency and Accountability; Due Diligence; Individual Participation; Security</p>
<p>Section 2: Agencies must complete the annual privacy assessment survey conducted by the Office of Privacy and Data Protection as part of the annual certification process. See Technology Policies, Standards, and Procedures (7.b.)</p>	<p>Govern</p>	<p>Transparency & Accountability, Lawful, Fair & Responsible Use</p>
<p>Section 3: Agencies must designate a privacy contact.</p>	<p>Identify</p> <p>Aligns with: NIST Privacy Framework ID.BE-P</p>	<p>Transparency & Accountability, Lawful, Fair & Responsible Use</p>

Links to Resources



- [Example Privacy Policy](#)
- [Privacy Notice Implementation Guidance](#)
- [Policy Crosswalk](#)
 - [Privacy Framework for State Agencies](#)
 - [Washington State Agency Privacy Principles](#)
- [Washington's Privacy and Data Protection Policy Webinar](#)
 - [Webinar Slide Deck](#)

Questions?

privacy@watech.wa.gov

www.watech.wa.gov/privacy