Data Privacy Guidelines

Document No: CDO-002
Updated: December 8, 2024
Issued by: Chief Data Officer

1.0 Purpose

The purpose of the Data Privacy Guidelines is to establish common guidelines for data privacy management across State of Hawaii agencies. Through responsible data privacy practice, State agencies can better serve citizens of the State of Hawaii while protecting privacy, managing risk, and promoting accountability and equity.

2.0 Authority

Hawaii Revised Statutes (HRS)[1] Section §27-44, established within the Office of Enterprise Technology Services, in the Department of Accounting and General Services, and under the authority of the Chief Information officer, the Chief Data Officer to develop, implement, and manage statewide data policies, procedures, standards, and guidelines. HRS §27-44 also established a Data Task Force to assist the Chief Data Officer in developing the State's data policies, procedures, and standards.

3.0 Scope

3.1. State Agencies

The Data Privacy Guidelines are developed with reference to the National Institute of Standards and Technology (NIST) Privacy Framework CORE.[2] It applies to all executive branch departments, including the Department of Education and the University of Hawaii, to ensure that we have common guidelines to protect data privacy across state agencies.

The Data Privacy Guidelines provide high level guidelines on data privacy protecting Personally Identifiable Information (PII) data. Each agency shall develop additional policies and guidelines as necessary according to relevant federal and state laws and regulations, both

[1] HRS §27-44. https://www.capitol.hawaii.gov/hrscurrent/Vol01_Ch0001-0042F/HRS0027/HRS_0027-0044.htm

[2] NIST Privacy Framework. https://nvlpus.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf

at the data set level and at the individual field level, to ensure compliance in its operations. When a conflict exists between the Data Privacy Guidelines and an agency's policy, the more restrictive policy will take precedence.

3.2 Definitions

The Data Privacy Guidelines provide guidelines for using Personal Identifiable Information (PII)[3] in data and Artificial Intelligence (AI) [4] processes.

3.3 Covered Use

The Data Privacy Guidelines apply to the handling of PII data in all data sets managed by state agencies, regardless of whether it is used for AI or not. This includes but is not limited to systems in the cloud, on premises, and on local drives.

The Data Privacy Guidelines shall be applied to the entire data life cycle from data creation, data collection, data cleansing and transformation, data storage and modeling, data science and analytics, data visualization, impact tracking, to data retention. It shall also be applied to all data applications, including Machine Learning[5] and AI.

4.0 Information Statement

4.1 Data Collection

- Data Minimization: Collect and process only the data absolutely needed for specific purposes. No extra PII data shall be collected. This reduces the amount of PII data stored and minimizes the potential for misuse.
- Authorization and Consent*:* Obtain consent required by law before collecting, using, or disclosing PII data. Provide clear and concise information about data usage, sharing, and options for withdrawing consent. If a data processor requests to re-purpose collected PII data, seek consent for that new use. This does not apply to open data and other non-private data. Maintain documented procedures for authorizing data processing activities, including internal approvals and individual consent mechanisms.
- Expressing Data Preferences: State agencies shall provide mechanisms for individuals to express their preferences on how their PII data is collected and used. This may include options to opt out of certain data collection practices or to limit how their PII data is shared with third parties.

[3] Refer to 7.0 Definitions of Key Terms
[4] Refer to 7.0 Definitions of Key Terms
[5] Refer to 7.0 Definitions of Key Terms

- Transparency: State agencies must provide clear and transparent notices on what data is being collected, the purpose of its collection, and how it will be used, to ensure compliance with relevant state and federal laws.

4.2 Data Processing and Sharing

- Accessing and Managing Data: If possible, allow individuals to have the right to request access to their PII data, review it for accuracy, and request deletion, following applicable legal requirements and data retention policies.
- Data Ownership and Accountability: State agencies shall identify data owners for each data set that contains PII information to promote accountability. Any use of PII data shall be in compliance with all federal, state, and local policies and regulations. No PII data shall be used in any GenAI model.
- Segregation and Access Controls: State agencies shall segregate PII data from public records and establish access controls according to all policies, laws, and regulations.

4.3 Data Protection

- Safeguards: State agencies shall implement appropriate safeguards, according to all federal and state laws and regulations, to protect PII data from unauthorized access, disclosure, alteration, or destruction. This includes security best practices, access controls, data encryption, and secure maintenance practices.
- De-identification and Pseudonymization: State agencies shall employ techniques such as de-identification (removing identifiers) and pseudonymization (replacing identifiers with unique codes) to limit the ability to identify individuals. This practice reduces the risk of individuals being singled out from the data set.

5.0 Compliance

The Data Privacy Guidelines shall take effect upon publication. The Chief Data Office may amend at any time; compliance with guidelines is strongly recommended to protect state PII data.

6.0 Contact Information

Submit all inquiries and requests for future enhancements to the Chief Data Officer in the Office of Enterprise Technology Services, Department of Accounting and General Services, at data@hawaii.gov.

All Data related policies and guidelines documents can be found at data.hawaii.gov.

7.0 Definitions of Key Terms

All terms shall have the meanings found in the Data & AI Glossary (under Glossaries on https://data.hawaii.gov/).

- **Data Privacy**: Data privacy refers to freedom from intrusion into the private life or affairs of an individual when that intrusion results from undue or illegal gathering and use of data about that individual.[6]
- **Access Control:** Access Control refers to the process of granting or denying specific requests to 1) obtain and use information and related information processing services and 2) enter specific physical facilities (e.g., federal buildings, military establishments, border crossing entrances).[7]
- **Personally Identifiable Information** (PII): Personally identifiable information refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.[8]
- **De-identification:** De-identification refers to any process of removing the association between a set of identifying data and the data subject.[9]
- **Pseudonymization:** Pseudonymization refers to a de-identification technique that replaces an identifier (or identifiers) for a data principal with a pseudonym in order to hide the identity of that data principal.[10]
- **Artificial Intelligence (AI):** A branch of computer science devotes to developing data processing systems that perform functions normally associated with human intelligence, such as reasoning, learning, and self-improvement.[11]
- **Machine learning (ML): Machine learning** refers to a field within artificial intelligence, focuses on the ability of computers to learn from provided data without being explicitly programmed for a particular task.[12]

8.0 Revision History

Date	**Description of Change**
December 16,2024	Approved by the State Data Task Force

[6] National Institute of Standards and Technology (NIST) SP 800-188. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-188.pdf

[7] National Institute of Standards and Technology (NIST) FIPS PUB 201-3. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-3.pdf

[8] OMB Circular A-130. https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf

[9] National Institute of Standards and Technology (NIST) Glossary. https://csrc.nist.gov/glossary/term/de_identification

[10] National Institute of Standards and Technology (NIST) Glossary. https://csrc.nist.gov/glossary/term/pseudonymization

[11] U.S. Department of State. https://www.state.gov/artificial-intelligence/#:~:text=Artificial%20Intelligence%20and%20Society&text=%E2%80%9CThe%20term%20'artificial%20intelligence',influencing%20real%20or%20virtual%20environments.%E2%80%9D

[12] National Institute of Standards and Technology (NIST). https://www.nccoe.nist.gov/ai/adversarial-machine-learning

9.0 Related Documents

[1] Information Quality Act (IQA). https://www.govinfo.gov/content/pkg/PLAW-106publ554/html/PLAW-106publ554.htm

[2] Children’s Online Privacy Protection Act (COPPA) — PII of children under 13. https://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-section6501&edition=prelim

[3] Critical Infrastructure Information, 6 USC CHAPTER 1, SUBCHAPTER XVIII, Part B. https://www.cisa.gov/sites/default/files/publications/CII-Act.pdf

[4] Driver's Privacy Protection Act (DPPA) H.R.3365 — 103rd Congress (1993-1994). https://www.law.cornell.edu/uscode/text/18/2721

[5] Family Educational Rights and Privacy Act (FERPA). https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

[6] Health Insurance Portability and Accountability Act of 1996 (HIPAA). https://aspe.hhs.gov/reports/health-insurance-portability-accountability-act-1996

[7] Privacy Act of 1974, 5 U.S.C. 552a. https://www.govinfo.gov/content/pkg/USCODE-2018-title5/pdf/USCODE-2018-title5-partI-chap5-subchapII-sec552a.pdf

[8] Criminal Justice Information Services (CJIS) Security Policy. https://le.fbi.gov/cjis-division/cjis-security-policy-resource-center

[9] Internal Revenue Service Tax Information Security Guidelines for Federal, State and Local Agencies. https://www.irs.gov/privacy-disclosure/safeguards-program

[10] Medicaid Information Technology Architecture (MITA) 3.0. https://www.medicaid.gov/medicaid/data-systems/medicaid-information-technology-architecture/medicaid-information-technology-architecture-framework/index.html

[11] Nacha Operating Rules. ACH payment. https://www.nacha.org/newrules

[12] Payment Card Industry Data Security Standard (PCI DSS) v 3.2. https://www.pcisecuritystandards.org/document_library/?category=pcidss&document=pci_dss

[15] Hawaii State DOT, Motor Vehicle Drivers License and related offices. https://hidot.hawaii.gov/highways/files/2018/02/Privacy_Policy_Stmnt_mvso-12-12-2017.pdf

[16] Fair Information Practice Principles (FIPPs). Fair Information Practice Principles (FIPPs) | FPC.gov