# PERSONAL PRIVACY OVERSIGHT COMMISSION
# AUGUST 23, 2023

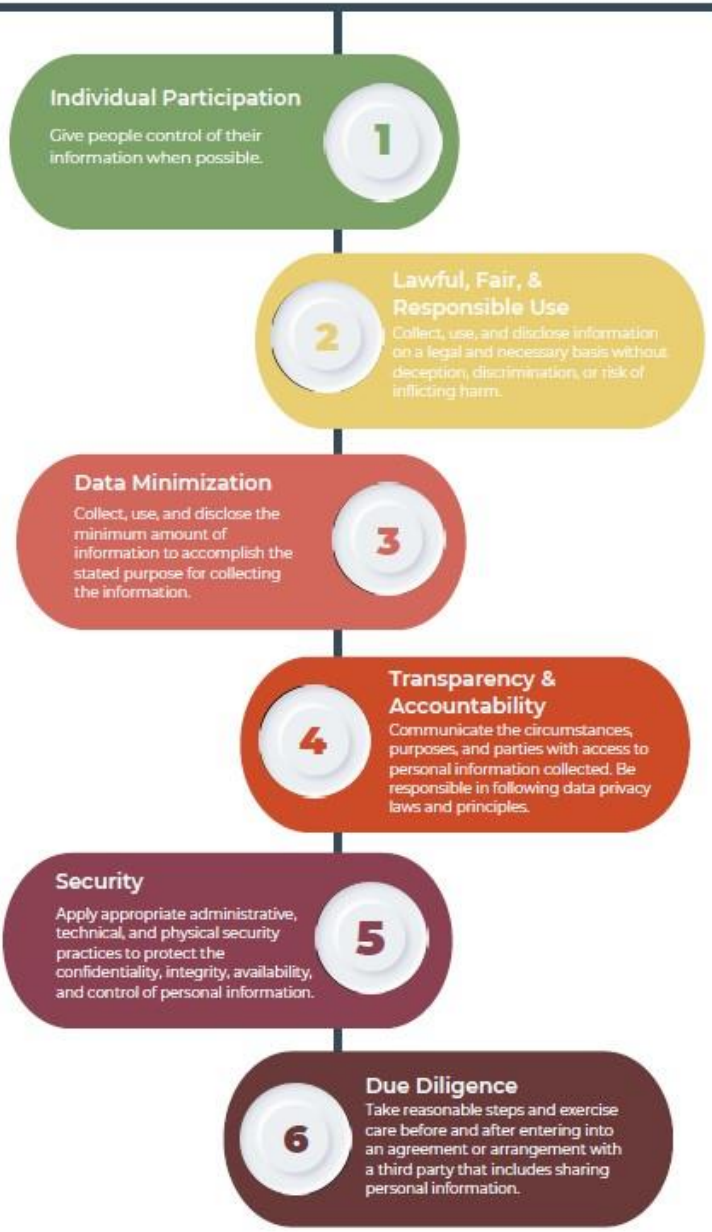
## DR. WHITNEY PHILLIPS, STATE PRIVACY OFFICER

OFFICE OF THE
STATE AUDITOR

# Agenda

1. Privacy Requirements for Government Entities
2. Privacy Law Definitions
3. Utah's State Constitution
4. Outline of PPOC Annual Report

# UTAH FUNDAMENTAL PRIVACY PRINCIPLES



| Principle | Topics | Recommendations | GRAMA | Governmental Internet Information Privacy Act | Privacy Protection Amendments (HB 243; 2021) | Cybersecurity Comission (HB 280;2022) | Cybersecurity Amendments (SB 127; 2023) | Consumer Privacy Act | UIPPA | HIPAA | FERPA | Student Privacy and Data Protection | Higher Education Student Data Protection (SB 226; 2022) | Protection of Pupil Rights Amendment | USBE Board Rule (R277-487) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Scope | | | All | All | All | All | All | Private | Private | Covered health care provider | Educational entities that recieve funding from the U.S. Department of Education | K-12 education | Public higher education | K-12 education | K-12 education |
| Individual Participation | Individual Participation | 1. Proposed government data privacy rights for Utah residents | 63G-2-601 Rights of individuals on | | | | | | | Summary of the HIPAA Privacy Rule | | | | | |
| | Opt/In opt-Out | | Can submit a notarized release of the | | | | | | | | 34 CFR § 99.37 - What conditions apply to disclosing directory information? 20 U.S. Code § | 53E-9-203(4) – (5) Makes PPRA more restrictive. | | 20 USC 1232h(c)(2) Development of | |
| | Fees | | 1. Must have a fee policy, 2. 63G-2-203: may | | | | | | | | | | | | |
| | Time Limitations | | (7) If one of the extraordinary | | | | | | | | | | | | |
| | Notice of Rights | | 1. 63G-2-205 Notice of Denial. 2. (2) | | | | | | | | Under FERPA, a school must annually notify eligible students of their rights under FERPA. The | | | | |
| | Notice of Appeal | | (1) (a) A | | | | | | | | | | | | |
| | Recordation | | If the government agency holding the private record | | | | | | | | 1. FERPA requires educational agencies and institutions to record all disclosures of PII from | | | | |
| | Access | | 63G-2-210 right to inspect a public record free | | | | | | | | An state education agency (SEA) or local education agency (LEA) must provide an eligible student | | | | |
| | Law Enforcement | | Limitations for those encarcerated; | | | | | | | | | | | | |
| | Voter Registration | | Voter Registration exception: (b) | | | | | | | | | | | | |
| | Expungement | | | | | | | | | | | 53E-9-306(1)(d) Using and expunging | | | R277-487-2(6) "Destroy" means to remove data or |
| | Notice of PII transfer | | | | | | | | | | Notice of record exchange after school transfer (often included in Annual FERPA Notice). | | | | |
| | Authorized Uses and Disclosure | | 63G-2-206 Effective 5/14/2019 | | | | | | | Authorized Uses and Disclosures | | | | | |
| | Other Provisions: Personal Representatives | | | | | | | | | Personal Representatives. The Privacy Rule | | | | | |
| | File Complaints | Add where individuals can file complaints within a Privacy Notice | 63G-2-205 Right of a notice of denial and a right | | | | | | | | Eligible students who believe that their FERPA rights may have been violated may file a complaint | | | | |
| | Process for amendment consideration | | 63G-2-304 Reight to appeal an access denial | | | | | | | | An SEA or LEA is required to consider the request for amendment, to inform the student | | | | |
| | Seek to amend | | 63G-2-603 Requests to amend a record | | | | | | | | Under FERPA, an eligible student has the right to seek amendment or correction of their education | | | | |
| | Privacy Notice for Data Collection | 1. Modify: change "privacy policy statement" to "privacy notice | Each governmental entity shall file | (2) A governmental website shall | | | | | | | | 53E-9-305(2) Requires USBE and LEAs to | | | |
| Data Minimization | Data Minimization | | 63G-2-604. Retention and disposition of | | | | | | | | | | | | Follow Retention Schedules; R277-487-4 De-identification R277-487: Public School Data |
| | Data De-identification | 1. Work on a quantitative de-identification scoring framework to ease | "summary data" means statistical records and | | | | | | | | | | | | |
| | Protected Information | | | | | | | | | What Information is Protected | | | | | |
| | Limiting Uses and Disclosures to the Minimum | | A government entity may dislose private | | | | | | | Minimum Necessary. A central aspect of | | | | | |
| | Annotation Requirement | | HB0343 (847-942) Utah Code | | | | | | | | | | | | |

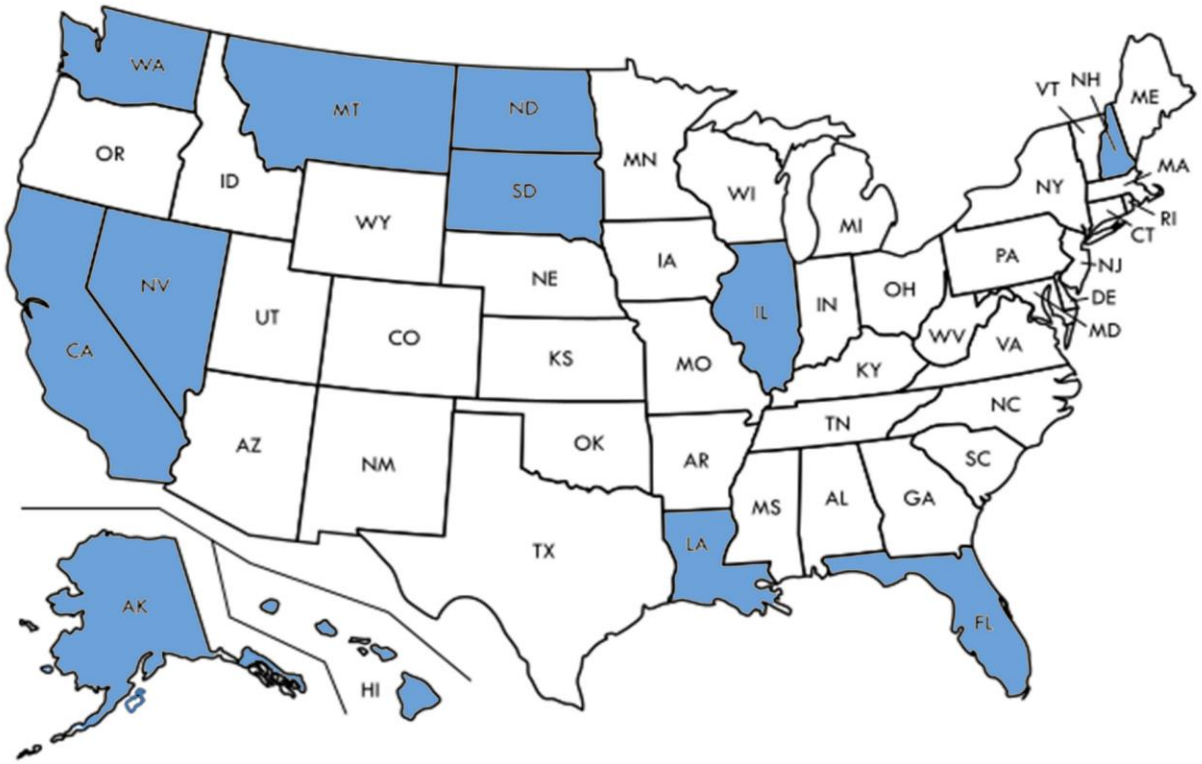
| Principle | Topics | Recommendations | GRAMA | Governmental Internet Information Privacy Act | Privacy Protection Amendments (HB 243; 2021) | Cybersecurity Comission (HB 280;2022) | Cybersecurity Amendments (SB 127; 2023) | Consumer Privacy Act | UIPPA | HIPAA | FERPA | Student Privacy and Data Protection | Higher Education Student Data Protection (SB 226; 2022) | Protection of Pupil Rights Amendment | USBE Board Rule (R277-487) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Security | Security | 1. All government entities that collect or maintain PERSONAL DATA must | | | | 63C-25-202. Commission duties. | | | | Summary of the HIPAA Security Rule | "reasonable security" | | | | Implement the CIS controls or a comparable IT |
| | Breach Investigation | | | | | | 13-44-202. Personal information -- | | | | | | | | R277-487-2(17) "Significant data breach" means a |
| | Breach Notification | Breach notification requirement similar to UCPA. | | | | | 13-44-202. Personal information -- (c) If an investigation under Subsection (1)(a) | SB227 (Utah Consumer Privacy Act) | 13-44-2-202 (UPPIA) Personal | Breach Notification Rule | | 53E-9-304(2)(a) Student data ownership and | | | Ensure that parents, eligible students, and |
| | Breach Reporting | | | | | | | | | | | 53E-9-3-304 Student data ownership and | | | R277-487-3(12) An LEA shall report all |
| | Data Classification | | 1. Each ordinance or policy relating to | | | | | | | | | | | | |
| | Physical Safeguards | | | | | | | | | Facility Access and Control. A covered entity | | | | | |
| Transparency & Accountability | Technical Safeguards | | | Beginning January 1, 2025, a governmental | | | | | | Access Control. A covered entity must implement | | | | | |
| | Transparency & Accountability | | 63F-2-204 (3) A governmental entity may make | | | 194 63C-25-205. Reporting | | | | | | | | | |
| | Notice and Other Individual Rights | | 63G-2-204 Right to be informed which | | | | | | | Privacy Practices Notice. Each covered entity. | | | | | |
| | Compliance & Enforcement | | Subdivision need to send their policies to the | | | | | | | HIPAA Compliance and Enforcement | | | | | |
| | Scope | | | | | | | | | | "Education records" | | | | |
| | Training | Incorporate: existing requirement to provide annual training to all staff | 63G-2-1-108 Certification of records officer. | | | | | | | Training Materials | | Provide annual training to all staff that have access | | | |
| | Privacy Advisory Groups | 7.1.1. Creation of a PPOC sub-group, the public safety privacy | | | HB243, 45-145 (2021) This bill creates | Cybersecurity Commission and Cybersecurity | | | | | | Three Advisory Groups: 1. Student data | 53B-28-5-502(1)-(3) State student | | |
| | Organizational Hierarchy | Creation of a Public Safety Privacy Officer position. | Chief Administratove Officer (CAO): 1. | | 1. Personal Privacy Oversight Comission | | | | | | The Student Privacy Policy Office (SPPO) leads the U.S. Department of Education's | 1. Create privacy officer within the Utah State Board | 53B-28-503. 1. Creates Privacy in Higher | | |
| | Penalties | | https://le.utah.gov/xcode/Title63G/ | | | | | SB227 (Utah Consumer Privacy Act) | | | Withholding federal funding; corrective action. | 53E-9-310 Penalties. | 53B-28-506 Penalties. | | |
| Due Diligence | Due Diligence | | "Notice of Compliance" means a | | | | | | | | | | | | |
| | Third-party contractor requirements | Add: 1. Certification of data destruction after agreement expiration. 2. | Must secure a written statement of the | | | | | | | Covered Entity Responsibilities. If a covered | 1.The party disclosing the PII from education records a Must enter into a written agreement to | Metadata Dictionary 53E-9-3-309 | 53B-28-5-505 Third-party contractors: | | |
| | Administrative Requirements | | (6) Before releasing a private. | | | | | | | HHS recognizes that covered entities range | | | | | |
| | Administrative Requirements | | | | | | | | | Security Management Process. As | | | | | |
| Lawful, Fair, & Responsible Use | Lawful, Fair, & Responsible Use | Prohibition on Monetization | A governmental entity shall disclose a record | | | | | | | | Generally, FERPA requires written consent from parents or "eligible students" (students who | | | | |
| | Sharing data | 1. Require creation of privacy risk register and use of PIAs. 2. Have a | Balance "any personal privacy interests. | | | | | | | | FERPA C.F.R. 99, Subpart D, May an Educational Agency or Institution Disclose Personally | 53E-9-308 Sharing student data -- | | | |
| | Research data sharing | | (8) (a) Except as provided in | | | | | | | | | | | | |
| | Data Governance Plan | 1. Refer to existing incorporate existing data governance plan | 1. Each political subdivision may | | | | | | | | | 53E-9-3-303 Requires each LEA to publically | 53B-28-5-503. Requires each public institution | | |

# Privacy Law Definitions

- Inventory of existing definitions related to privacy
- Federal and state law, and administrative rule


Dates
Board
Reasonable
Governmental
Education
Token
Processor
Access
Committee
Data
Portal
Advisory
Record
Person
Government
Enforcement
Breach
Code
Individual
Hash
Protected
Stewardship
Funds
Management
employee
Educational
Email
Nonprofit
Healthcare
Personally
Biometric
XSS
Critical
Safety
State
Facility
Website
Schedule
Financial
Geolocation
Targeted
Student
Sponsored
Subdivision
Governance
Covered
Body
Request
Child
Address
Public
Privacy
Instructional
Audit
Plan
Party
Control
Authenticator
Cross
Suppression
Security
Business
Health
Chronological
Collected
Notice
Appointed
Utah
Local
Agency
Assessment
Agreement
Level
Mechanisms
Proceeding
Law
Identifier
Disclosure
Stewards
Private
Entity
Officer
Open
Provider
Attendance
Sanitization
Authorized
Administrative
Domain
Correctional
Chief
Information
Advertising
Transfer
Higher
Program
Identifiable
Limitation

# Privacy in U.S. State Constitutions



# PPOC Annual Report

1. **Risk Classification:** a comprehensive evaluation and description of the risk formula we used to classify government entities by risk. The formula includes a) number of employees, b) number of constituents, and c) sensitivity of data

2. **Compliance of the following:**
   a. **Privacy Policy Statement:** a comprehensive evaluation of which government entities are fully, partially, or not compliant with 63D-2-103.
   b. **Certified Records Officers:** percent of government entities with a certified records officer as described in 63G-2-108.
   c. **K-12 Public Education:** an evaluation of specific requirements required by federal, state law, and board rule listed here.
   d. **Institutions of Higher Education:** an evaluation of the specific requirements listed here.

3. **Training and Awareness Campaign:** a description of the trainings performed in FY23 including a) topic, b) intended audience, c) estimated number of participants, d) and related federal or state privacy requirements.

4. **Privacy Health Checks:** review of the administrative, physical, and technical safeguards of specific government entities. This includes reviews of entities that are at all levels of risk classification. This includes the development of a Privacy Impact Assessment (PIA) tool.

5. **Legislation:** a list of all 2023 bills that were reviewed for privacy consideration, as well as prioritized recommendations for 2024 legislative changes.