Privacy 101

Nora Kurzova
Asst. State Privacy Officer
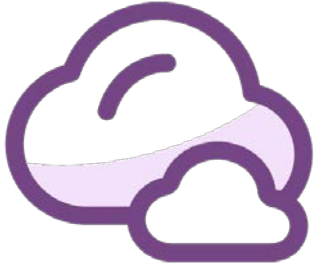**State of Utah**
January 9, 2024

Personal Data:

"Any information related to an identifiable individual."

slido

What is the difference between PERSONAL data and SENSITIVE personal data?

ⓘ Start presenting to display the poll results on this slide.

"Any information related to an identifiable individual, that is likely to cause **greater harm if abused**."

Utah Fundamental Privacy Principles

- **Individual Participation**
- **Lawful, Fair, and Responsible Use**
- **Data Minimization**
- **Transparency and Accountability**
- **Security**
- **Due Diligence**

Golden rules of privacy protection

- **"Limit"** - only collect what you truly need and only use it for the primary purpose for which the data was collected.

- **"Guard"** - protect the data from unauthorized access, online and offline.

- **"Delete"** - dispose of personal data when you no longer need it, review and follow retention schedules. Conduct clean desk exercises.

- **"No surprises"** - no data use should "surprise" the data subject (person)
- **"No hostages"** - data should be easily portable & erasable.

- **"Privacy by Design"** - consider privacy when new use of data is designed
- **"Privacy by Default"** - the default setting/use should be the most restrictive.

Over-Collection and Over-Retention

- Over-collection happens when we collect or "process" more data than actually needed.

- Over-collection thrives in old habits.

- Over-collection presents higher risk and goes against the "data minimization" principle.

- Over-retention means you keep data longer than needed.

- Over-retention increases risk as the data accumulates, and/ or becomes obsolete.

OFFICE OF THE
STATE AUDITOR

To Destroy or Not to Destroy?
How long to keep records

Dr. Whitney Phillips
State Privacy Officer
State of Utah
January 9, 2024

Questions

- Can I clean out that room with files going back to the dawn of time?

- How long should we keep records?

- How should we dispose of records?

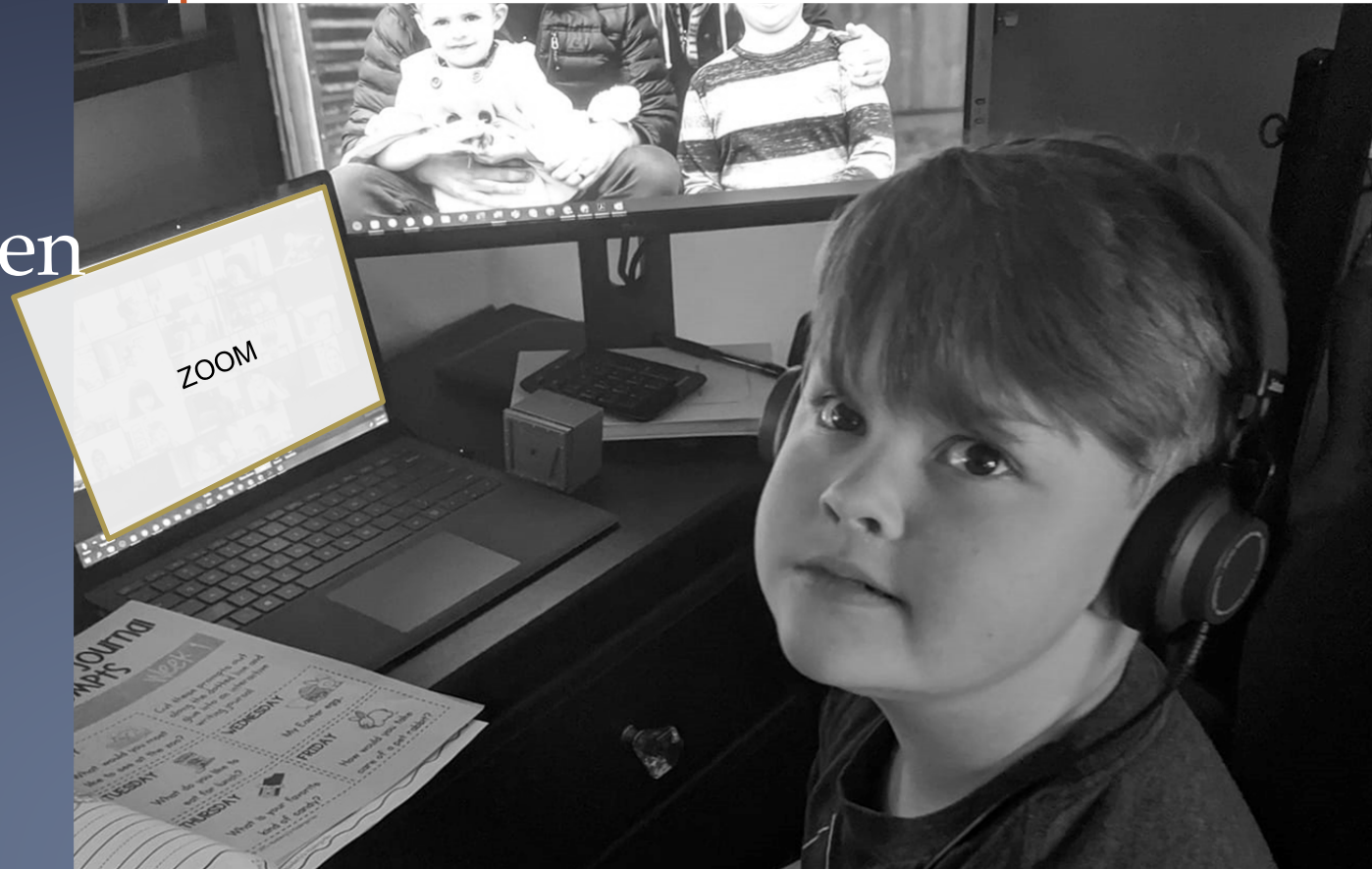- If we need to keep records, is there a place to store them?

OFFICE OF THE
STATE AUDITOR

BUT I NEED ALL THESE RECORDS!

East High
1920

Kindergarten in 2020

ZOOM

Certified Records Officers (R.O.) Metrics

Table 1. Summary of entities with a listed Records Officer by entity category, sorted by rate of compliance.

Entity Category	Number of Entities	Number of RO and %	
Public School	217	214	= 98.62%
County	243	238	= 97.94%
State Agency	749	699	= 93.32%
Municipality	499	441	= 88.38%
Associations of Government	8	7	= 87.50%
Charter School	142	122	= 85.92%
Special Service District	527	425	= 80.65%
Interlocal	24	18	= 75.00%
College or University	40	26	= 65.00%
Independent or Quasi-Government	19	9	= 47.37%
Other	20	8	= 40.00%
Local District	27	4	= 14.81%

https://archives.uutah.gov/rim/retention-schedules.html

OFFICE OF THE STATE AUDITOR

RECORDS APPRAISAL & MANAGEMENT PROGRAM

NON-RECORDS

- ITEMS OF NO LEGAL, ADMINISTRATIVE, FISCAL OR HISTORICAL VALUE
- DRAFTS
- ROUGH NOTES
- EXTRA COPIES

STATE ARCHIVES
801-531-3863
RECORDSMANAGEMENT@UTAH.GOV

ONE YEAR OR LESS

- ATTENDANCE ROLLS
- PERMISSION & PASSES
- STUDENT DISCIPLINE
- SURVEILLANCE RECORDINGS
- WORKING FILES
- INVENTORY RECORDS
- INTERNAL COMMITTEE RECORDS
- TRANSITORY CORRESPONDENCE

☑ DISPOSE 1 YEAR AFTER RESOLUTION, OR ISSUE IS SUPERSEDED

ONE TO SIX YEARS

- DEAD FILES (3)
- PAYROLL PROCESS (3)
- PERFORMANCE & TESTING (3)
- SECTION 504 STUDENT RECORDS (3)
- STUDENT MEDICAL LOGS (3)
- TIMEKEEPING (3)
- ACCOUNTS PAYABLE (4)
- BUDGET RECORDS (4)
- ENROLLMENT & REGISTRATION (4)
- SPECIAL EDUCATION RECORDS (5)

☑ SEE STATE ARCHIVES FOR SPECIFIC DISPOSITION SCHEDULE

MORE THAN 7 YEARS

- ADMINISTRATIVE CORRESPONDENCE (7)
- GRANT RECORDS (7)
- INVESTIGATION RECORDS (7)
- AUDIT WORK PAPERS (10)
- CIVIL CASE FILES (10)
- FIXED ASSETS (10)
- PROGRAM & PROJECT ANALYSIS (10)
- SCHOOL GENERAL LEDGERS (10)
- INSURANCE CLAIMS (12)
- EMPLOYEE WAGE RECORDS (65)

☑ SEE STATE ARCHIVES FOR SPECIFIC DISPOSITION SCHEDULE

PERMANENT

- ARTIFACTS
- AUDIT RECORDS
- SPORTS TEAMS RECORDS
- STUDENT ACADEMIC RECORDS
- CLOSED MEETING RECORDS
- GRADUATION & TRANSCRIPT
- GRADUATION PROGRAMS
- HISTORIAN BOOKS
- MEETING MINUTES
- OFFICIAL REPORTS
- PUBLIC MATERIALS
- PUBLIC RELATIONS
- PUBLICATIONS
- SCHOOL HISTORIES
- STUDENT HISTORY
- TRAINING AIDS

PLEASE REFER TO STATE ARCHIVES FOR SPECIFIC SCHEDULE LENGTHS, AND RECORD DISPOSITION NOTES. THIS IS DESIGNED TO BE A QUICK GLANCE GUIDE FOR THE MOST USED RECORD TYPES.

ADA Compliant 5/2021

< Go to Dashboard

Records Retention for Law Enforcement

0% complete

Search by lesson title ▼

○ **Course Outline**   0/3 ∨

○ **1 - Introduction**   0/2 ∨

○ **2 - Records Management**   0/4 ∧

○ **What is records management?**
   ▣ TEXT

○ What are Records?
   ▣ TEXT

○ Records Management -- the Special Case for Law Enforcement
   ▣ TEXT

○ Quiz 1 - Basics of Records Management
   ▣ QUIZ · 3 QUESTIONS · PREREQUISITE

What is records management?

Records information management or **RIM** is the "field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use, and disposition of records, including processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records."[1]

A records management program provides intellectual and physical control over the records produced, maintained, and disposed of by an entity in the course of fulfilling its business functions.

[1] ISO IS 15489-1:2001(E): Information and documentation – Records management – Part 1: General, 3.16. International Organization for Standardization, Geneva, Switzerland, 3.

COMPLETE & CONTINUE →

Records Retention for Law Enforcement

0% complete

Search by lesson title

- ○ **Course Outline** 0/3 ⌃
  - ○ Course Outline
    📄 TEXT
  - ○ Sample audio file.
    🔈 AUDIO
  - ○ Sample video
    📹 VIDEO · < 1 MIN
- ○ **1 - Introduction** 0/2 ⌄
- ○ **2 - Records Management** 0/4 ⌄
- ○ **3 - Records Retention Basics** 0/3 ⌄
- ○ **4 - Records Retention Step-by-Step** 0/17 ⌄
- ○ **Conclusions** 0/1 ⌄
- ○ **Final Quiz - Records Retention for Law Enforcement** 0/1 ⌄
- ○ **Next steps** 0/2 ⌄
- ○ **Video Resources** 0/5 ⌄

Course Outline

Course outline

Section One

Introduction - This section will introduce basic concepts such as what is "information" in a records retention setting.

Section Two

Records Management - This section will introduce the basics of what state law requires and best practices for managing departmental records. Refresher quiz.

Section Three

Records Retention Basics - This section will introduce what records retention is and obligations of state/municipal employees,

Section Four

Records Retention Step-By-Step - This section takes a deeper dive into how employees can best fulfill their obligations, what record retentions schedules are, and how to employ best practices. Refresher quiz.

Conclusions

A brief summation of the course.

*There will be a 15 question quiz where an 80% score or higher should give you confidence to seek certification through the Utah Division of Archives and Records Service.

Next Steps

Last statements, links to additional study resources and Archives' certification test.

Video Resources

Videos that offer an overview of GRAMA and PRMA legislation, retention and scheduling best practices. (*One may wish to review these first, though they will probably make more sense afterwards.*)

COMPLETE & CONTINUE →

So, what do I want you to do?

1. Make sure that you have a certified Records Officer.

2. Learn the joy of destroying records (legally)

3. Test the Record Retention for Law Enforcement course

Contact info

- Heidi Steed, Local Government RIM Consultant (801) 531-3860
hsteed@utah.gov

AI and Privacy

Nora Kurzova
Asst. State Privacy Officer
State of Utah
January 9, 2024

OFFICE OF THE
STATE AUDITOR

Lets Talk About AI

- **What AI are we talking about?**

  "Narrow / Weak AI" (including generative AI), AI that is not "general", not self-aware, not surpassing the capability of a human mind.

- **Why do we care?**

  If used incorrectly, it can present variety of bias, lead to skewed results, become intrusive or manipulative, or aid criminals.

OFFICE OF THE
STATE AUDITOR

Common privacy concerns people raise against AI

- I find it intrusive

- I find it unexpected

- I find it non transparent

- I think it manipulates me

- I cannot control its settings

- I think it discriminates against me

- The data can leak/be stolen and abused

- It harvests my data and sells it onward

What can you do to aleviate these concerns?

- I find it intrusive – Privacy Impact Assessment
- I find it unexpected – Privacy notice
- I find it non transparent – Privacy policy
- It manipulates me – Ethical use of Data Policy
- I cannot control its settings – Privacy by D&D
- It discriminates – PIA with extra Bias Check
- It harvests my data and sells it onward – Ban on Monetization (or exchange) of the data.
- The data can leak/be stolen and abused – PIA, and a retention policy with enforced deletion.

OFFICE OF THE
STATE AUDITOR

Incident Response:

- Data Incident: unauthorized or unintended event that compromises the confidentiality, integrity, or availability of data. It includes both accidental and intentional incidents.

  – Example: power outage causing systems to be down/data unavailable, lost computer, sensitive documents left at a printer,

- Data breach: actual unauthorized access, acquisition, or disclosure of sensitive, confidential or personal, protected or otherwise controlled data.

  – Example: computer was unencrypted and stolen by a bad actor who accessed personal data stored on it, recipient opened the attachment, colleague who didn't have a need to know reviewed the document.

- EVERY BREACH IS AN INCIDENT, NOT EVERY INCIDENT IS A BREACH.

OFFICE OF THE
STATE AUDITOR

Incident Response basic rules:

- **BASIC RULES FOR BEFORE AN INCIDENT:**
  - Have a documented incident response plan, (that includes incident classification, escalation points and path to communicate securely.)
  - Know who to contact and bring in when there is an incident (IT, Legal, Communications..)
  - Teach people to recognize and report incidents, but not to "classify" or "resolve" them unless they are properly trained to do so.
  - Measure progress periodically.
- **BASIC RULES FOR DURING AN INCIDENT:**
  - Act swiftly: Bring in experts to respond to data incident and mitigate it promptly.
  - Communicate openly and effectively: Maintain clear communication channels with stakeholders
  - Document your steps.

Incident Response basic rules:

- **BASIC RULES FOR AFTER AN INCIDENT:**

  - Uphold your legal obligations towards affected people and regulators.

  - Learn and improve: Conduct thorough post-incident analysis to identify weaknesses, implement necessary changes, and enhance future incident response capabilities.

  - Train, test, monitor.

Incident Response basics:

MOST COMMON INCIDENTS CAUSED BY HUMAN ERROR:

- **Accidental data exposure**: Sending information to the wrong recipient via email.

- **Misconfigured privacy setting**s: Incorrectly configuring access controls, leading to unauthorized data access, poor identity management.

- **Lost or stolen devices:** Misplacing or theft of devices containing sensitive data.

- **Improper data disposal:** Failure to properly destroy or wipe physical or electronic data before disposal.

- **Weak passwords and credentials:** Using weak passwords or sharing credentials increases the risk of unauthorized access.

Incident Response Takeaways

- Have an Incident Response Plan in place and review it annually.

- Engage experts - cyber, privacy, legal.

- Train, test, monitor - everybody.

Lets watch and learn

Can you identify some of the things this group of "responders" did wrong?

https://www.exterro.com/how-a-small-data-breach-can-lead-to-big-compliance-risks

2024 Proposed Legislation

Dr. Whitney Phillips
State Privacy Officer
State of Utah
January 9, 2024

OFFICE OF THE STATE AUDITOR

2024 Legislative Session

OFFICE OF THE
STATE AUDITOR

Potential privacy legislation

- Government Privacy Act

- AI

The big 3:

- Public Safety

- Education (minors)

- Health (physical and mental)

Potential privacy legislation

- Government Privacy Act
- AI

The big 3:
- Public Safety
- Education (minors)
- Health (physical and mental)