Keeping Our History Safe: Simple Steps to Protect Our Digital Archive

xAI Development Team

May 5, 2025

1 A Promise to Protect Our Stories

Our historical society holds a treasure trove of photographs, documents, and videos—each one a piece of our shared past. But some of these treasures, like donor names or personal stories, are sensitive and need extra care. Think of our digital archive as a museum vault: we need strong locks and clear rules to keep everything safe. Our smart storage system (called software-defined storage, or SDS) organizes artifacts into "Hot," "Warm," and "Cold" shelves, making it easier to manage. This report explains the laws we must follow to protect sensitive information and shares practical ways to keep our archive secure, so we can focus on preserving history while earning the trust of our community.

2 The Rules We Need to Follow

Some of our artifacts contain private details, like a donor's address or a medical story in an oral history. These are protected by laws that ensure we handle them responsibly. Here's a simple breakdown of the key rules that apply to our archive:

- European Privacy Rules (GDPR): If we have data from European donors or records, we need their permission to store it, must let them see or delete it, and have to keep it super secure—like locking it in a safe. We also need to report any break-ins within 3 days. Breaking this rule could cost millions.
- California Privacy Law (CCPA): For California donors, we must tell them what data we collect, let them say "don't share it," and protect it from hackers. Mistakes could cost $7,500 per person affected.
- Health Data Rules (HIPAA): If we have medical details, like someone's health history in a video, we need to restrict who sees it, lock it tightly, and track every access. Violations could cost $250,000.
- Canadian Privacy Law (PIPEDA): For Canadian donors, we need their okay to store data, must keep it safe, and let them check it. Fines could reach $80,000.
- Payment Security Rules (PCI DSS): If we store donor credit card info, we should avoid keeping sensitive bits (like card codes) and lock up what we do keep. Breaking this could cost $100,000 a month.

- Financial Record Rules (SOX): For our financial records, like donation logs, we must keep them for 5 years and make sure they can't be changed. Mistakes could lead to big fines or legal trouble.

These laws all say similar things: lock up private data, control who sees it, track access, delete data when it's not needed, report problems fast, store data in the right places, and be open about what we do. Following them keeps our archive safe and our reputation strong.

3 Why These Rules Matter to Us

Our archive likely includes:

- Personal Details: Names or addresses in donor records, covered by European, California, or Canadian privacy laws.
- Health Stories: Medical details in oral histories, protected by health data rules.
- Payment Info: Credit card details from donations, needing payment security.
- Financial Logs: Records of contributions, covered by financial rules.

If we don't follow these laws, we could face huge fines, lose donor trust, or even face lawsuits. Our SDS system, which saved us $117,750 over 5 years compared to old-style storage, can help us follow these rules without breaking the bank.

4 How We'll Keep Our Archive Safe

Here are simple, practical ways to make our SDS system secure and follow the law, like adding locks, keys, and a security guard to our digital museum.

4.1 Lock Data with Strong Encryption

- What: Use a digital "lock" (called AES-256 encryption) to scramble all artifacts so only authorized people can read them. Use another lock (TLS 1.3) when sending data over the internet.
- Why: Every law says we must protect private data from hackers.
- How: Set up our cloud storage (like AWS) to automatically lock data and use secure connections for access.
- Win: Keeps sensitive donor details or health stories safe, even if someone tries to break in.

4.2 Give Access Only to the Right People

- What: Create "keys" so only certain staff can access certain artifacts—like only archivists see Hot or Warm data, and only managers see everything.
- Why: Laws say we must limit who can see private data to avoid leaks.

- How: Add a system to our SDS (like digital ID cards) to check who's allowed to access what.
- Win: Stops unauthorized access, keeping donor trust intact.

4.3 Keep a Log of Who Looks at Data

- What: Track every time someone accesses or changes an artifact, like a guestbook showing who visited the vault.
- Why: Health, payment, and financial rules require us to know who's touching sensitive data.
- How: Add a logging feature to our SDS system to record actions, using tools in our cloud setup.
- Win: Helps us spot problems and prove we're following the rules during inspections.

4.4 Clean Up Old Data Automatically

- What: Decide how long to keep data (e.g., 5 years for financial records) and automatically delete it when it's time, like clearing out expired files.
- Why: Privacy laws say we shouldn't keep data longer than needed.
- How: Update our SDS to tag artifacts with "keep until" dates and let the system delete them.
- Win: Saves storage space and keeps us out of legal trouble.

4.5 Be Ready for Break-Ins

- What: Have a plan to spot a data break-in, tell affected people within 3 days, and fix the problem fast.
- Why: Privacy laws require quick action to protect people.
- How: Use cloud tools to watch for suspicious activity and write a step-by-step response plan.
- Win: Limits damage and shows we're responsible.

4.6 Store Data in the Right Places

- What: Keep data in regions where it's legally allowed—like European data in Europe.
- Why: Some laws say data can't cross borders without special rules.
- How: Set our SDS to store data in specific cloud regions (e.g., Germany for European data).
- Win: Avoids fines for storing data in the wrong place.

4.7 Tell Everyone How We Protect Data

- What: Write a clear "privacy promise" explaining how we handle data—like saying, "We lock up your details and only keep them as long as needed."
- Why: Privacy laws require us to be open with donors and visitors.
- How: Work with a lawyer to create a policy and post it on our website.
- Win: Builds trust and shows we're doing things right.

4.8 Train Our Team and Check Partners

- What: Teach our staff how to handle data safely and check that our tech partners (like cloud providers) follow the rules.
- Why: Many breaches happen because of human mistakes or sloppy partners.
- How: Hold yearly training sessions and review our cloud provider's certifications.
- Win: Keeps our team sharp and our partners accountable.

5 Fitting These Steps into Our SDS System

Our SDS system, with its smart organization and cloud setup, is perfect for these protections:

- Smart Tagging: Update our system to label artifacts as "sensitive" (e.g., donor data) and set expiration dates, so they're stored and deleted correctly.
- Safe Access: Add locks and logs to our data retrieval process, building on our speed tests that showed fast access times (around 85 milliseconds).
- Cloud Helpers: Use our cloud provider's tools (like AWS's security features) to handle encryption, logging, and monitoring without extra cost, keeping our budget at $187,500 over 5 years.
- Easy Automation: Let the system handle cleanup and monitoring, so our staff can focus on history, not paperwork.

6 Let's Keep Our Archive Safe and Trusted

Protecting our digital archive isn't just about following laws—it's about honoring the trust of everyone who shares their stories with us. By adding strong locks (encryption), limiting access (keys), tracking visits (logs), cleaning up old files, preparing for problems, storing data correctly, being open, and training our team, we'll keep our archive safe and legal. These steps fit right into our SDS system, keeping costs low and work simple. Let's make these changes to protect our history and our community for years to come.