Library Privacy and Vendor Management II: Exploring Practical Strategies and Best Practices

Part of the PLP Data Privacy Best Practices Training for Libraries Project

May 2020
This project was supported in whole or in part by the U.S. Institute of Museum and Library Services under the provisions of the Library Services and Technology Act, administered in California by the State Librarian. The opinions expressed herein do not necessarily reflect the position or policy of the U.S. Institute of Museum and Library Services or the California State Library, and no official endorsement by the U.S. Institute of Museum and Library Services or the California State Library should be inferred.

This document does not constitute legal advice, and is for informational purposes only. Please consult an attorney or other legal counsel for legal advice.

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

Cover Page Photo Credit - Privacy by Nick Youngson CC BY-SA 3.0 ImageCreator

Handbook developed by Becky Yoose, LDH Consulting Services 
becky@ldhconsultingservices.com
Table of Contents

Acronyms.............................................................................................................................................................1
Patron Data Lifecycle Quick Reference Map........................................................................................................2
Vendor Relationship Lifecycle Quick Reference Map................................................................................................3
Exercises..................................................................................................................................................................4
Slides....................................................................................................................................................................6
References, Further Reading, and Example Sources..............................................................................................14
# Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALA</td>
<td>American Library Association</td>
</tr>
<tr>
<td>CalOPPA</td>
<td>California Online Privacy Protection Act of 2003</td>
</tr>
<tr>
<td>CCPA</td>
<td>California Consumer Privacy Act</td>
</tr>
<tr>
<td>COPPA</td>
<td>Children’s Online Privacy Protection Act</td>
</tr>
<tr>
<td>FERPA</td>
<td>Family Educational Rights and Privacy Act</td>
</tr>
<tr>
<td>GDPR</td>
<td>General Data Protection Regulation</td>
</tr>
<tr>
<td>IANAL</td>
<td>I Am Not A Lawyer (always a good acronym to have in your back pocket!)</td>
</tr>
<tr>
<td>ISO</td>
<td>International Organization for Standardization</td>
</tr>
<tr>
<td>NDA</td>
<td>Non-Disclosure Agreement</td>
</tr>
<tr>
<td>NIST</td>
<td>National Institute of Standards and Technology</td>
</tr>
<tr>
<td>PII</td>
<td>Personally Identifiable Information</td>
</tr>
<tr>
<td>RFI</td>
<td>Request For Information</td>
</tr>
<tr>
<td>RFP</td>
<td>Request For Proposals</td>
</tr>
</tbody>
</table>
# Patron Data Lifecycle Quick Reference Map

<table>
<thead>
<tr>
<th>Phase</th>
<th>Question</th>
<th>Best Practice</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collection</td>
<td>What patron data are you collecting, and why?</td>
<td>Only collect data needed for demonstrated business cases</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Practice “The Five Whys”</td>
</tr>
<tr>
<td>Storage</td>
<td>Where is the patron data stored?</td>
<td>Limit number of data storage areas</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Limit storage of patron data in local and vendor systems</td>
</tr>
<tr>
<td>Access</td>
<td>Who has access to the patron data?</td>
<td>Limit physical and electronic access to data</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Audit vendor security and privacy practices</td>
</tr>
<tr>
<td>Reporting</td>
<td>What patron data is published to staff and to the public?</td>
<td>Aggregate data and control access to data through dashboards, database views, and other data reporting tools</td>
</tr>
<tr>
<td>Retention</td>
<td>How long is patron data kept?</td>
<td>Follow local and state retention regulations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Ensure backups and logs are covered in retention policies</td>
</tr>
<tr>
<td>Deletion</td>
<td>How is patron data deleted?</td>
<td>Properly dispose of physical and electronic media that contained patron PII</td>
</tr>
<tr>
<td>Phase</td>
<td>Best Practices and Tools</td>
<td></td>
</tr>
<tr>
<td>--------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
</tbody>
</table>
| Selection          | Use Request for Information (RFI) to gather information about general vendor privacy practices  
                      Include data privacy and security Functional Requirements in Request for Proposals (RFPs)                                                                                                               |
| Onboarding         | Plan strategies and identify compromise and dealbreaker items before starting contract negotiations  
                      Use contract addendums and non-disclosure agreements (NDAs)                                                                                                                                                  |
| Maintaining        | Schedule and conduct regular security and privacy audits  
                      Review impact on patron privacy of major changes in contract or product functionality and choose to either renegotiate the contract or non-renewal                                                                 |
| Separation         | Work with vendor to export and delete patron data when the business relationship ends                                                                                                                                 |

Vendor Relationship Lifecycle

Quick Reference Map

- **Selection**
  - Use Request for Information (RFI) to gather information about general vendor privacy practices
  - Include data privacy and security Functional Requirements in Request for Proposals (RFPs)

- **Onboarding**
  - Plan strategies and identify compromise and dealbreaker items before starting contract negotiations
  - Use contract addendums and non-disclosure agreements (NDAs)

- **Maintaining**
  - Schedule and conduct regular security and privacy audits
  - Review impact on patron privacy of major changes in contract or product functionality and choose to either renegotiate the contract or non-renewal

- **Separation**
  - Work with vendor to export and delete patron data when the business relationship ends
Exercises

Exercise – RFP Show & Tell
Review the RFP section assigned to your group and discuss the questions below. Assign a note taker and a person to report out to the entire group.

What does your RFP section cover with regard to privacy?

What is the main strength of your RFP section?

What is one way your RFP section can be improved in protecting patron privacy?
Exercise – Contract Flags

Every contract will include at least one flag, and there are many flags to watch out for. Here is a small list of important contract flags to look for when reading the contract with a privacy lens:

- “Reasonable” and use of other vague terms to describe privacy or security practices
- Lack of definitions for terms
- Termination of contract – no information about what happens to your library’s data after the business relationship ends
- Data ownership
- Lack of information about responses to law enforcement or government data requests
- Legal jurisdiction of the contract
- Lack of transparency in contract details
- Indemnity/liability clauses
- Data reselling or disclosure to other third parties
- Monitoring patron use (including web analytics)
- Using “Aggregated”, “Anonymized”, “De-identified” without defining methods

Review the RFP section assigned to your group and discuss the questions below. Assign a note taker and a person to report out to the entire group.

What red flags in the above list did you identify in the contract?

Were there any red flags not on the list that you found in the contract? If so, what were they and why would you consider them red flags?

Have you encountered these red flags at your library? If so, how did you address them with the vendor?
Library Privacy and Vendor Management II: Exploring Practical Strategies and Best Practices

Becky Yoose
Library Data Privacy Consultant, LDH Consulting Services
Pacific Library Partnership, May 2020

Workshop Housekeeping – Guidelines

- All responses and questions are valid.
- Assume good intent.
- When you disagree, challenge or criticize the idea, not the person.
- Be mindful of the time.
- One speaker at a time.
- Speak from your own perspective.
- Help protect others’ privacy by observing the Chatham House Rule.
Workshop Housekeeping - Logistics
IANAL; Consult legal staff for legal advice
Exercises and Discussions - what to expect
Toolkit tie-in
Privacy measures are only as strong as the least-knowledgeable person working with patron data

Section One:
Refresher on Vendors and Libraries

Library Patron Data Lifecycle

Library Privacy and Vendor Management II
Vendor Relationship Lifecycle

Selection

Separation

Onboarding

Maintaining

Section Two: Selection Best Practices and Strategies

Selection - Where to start?

**RFI - Request for Information**
- Used to gather information about services or products
  - Obtain privacy policies
  - Gather information about *general* privacy features

**RFP - Request for Proposals**
- Used to gather bids from potential vendors
  - Outline privacy reqs
  - Gather information about *specific* privacy features
Exercise – RFP Show & Tell

Section Three: Onboarding – ALL the Contracts

Contracts and Legal Regulations
• California Gov Code § 6267
• California Consumer Privacy Act of 2018 (CCPA)
• California Civil Code Section 1798.82
• Family Educational Rights and Privacy Act (FERPA)
• Children's Online Privacy Protection Act (COPPA)
• Local Regulations, including record retention schedules and public disclosure exemptions and regulations
• Parent institution policies or contract boilerplate
Onboarding – Privacy & Contract Red Flags

- “Reasonable” and vague terms
- Lack of definitions for terms
- Indemnity/liability clauses
- Termination details – data exit
- Lack of information about responses to law enforcement or government data requests
- Legal jurisdiction!
- Lack of transparency
- Data ownership
- Data reselling or disclosure to other third parties
- Monitoring patron use (web analytics)
- Using “Aggregated”, “Anonymized”, “De-identified” without defining methods

Exercise – Contract Flags

Onboarding - Contract Addendum and NDA

**Contract Addendum**
- Legal boilerplate for standard privacy and security contract language
- Can be used in both initial contract signings and renewal periods

**Non Disclosure Agreement**
- AKA NDAs
- Limit or prohibit sharing of patron data to:
  - Subcontractors
  - Service Providers
  - Other Third Parties

Library Privacy and Vender Management II

May 2020

Pg. 10
Walkthrough – Contract Addendum

Section 3.5 Communications

Onboarding – Communications

**Staff**
- Announcements via:
  - Email
  - Staff Intranet
  - Meetings
  - Vendor privacy notice list
  - Update privacy policies if necessary

**Patrons**
- Press releases or news announcements
- Vendor privacy notice list on public site
- Update privacy notice if necessary
Discussion – Public Communication Examples

Section Four: Maintenance Best Practices and Strategies

Walkthrough – Vendor Audit
Section Five: Wrap up

What is one thing from this workshop that you can put into practice or discussion at your library when you return?

Thank you :-)

Becky Yoose
Library Data Privacy Consultant
LDH Consulting Services
Email: becky@ldhconsultingservices.com

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.
References and Further Reading

General

https://digitalcommons.du.edu/cgi/viewcontent.cgi?article=1330&context=collaborativelibrarianship.


https://librarytechnology.org/repository/item.pl?id=20425.


Green, Ben Z., Gabe Cunningham, Ariel Ekblaw, Andrew Linzer, Paul M. Kominers, and Susan Patricia Crawford. 2017. “Open Data Privacy.”
https://dash.harvard.edu/handle/1/30340010.


https://doi.org/10.1080/1941126X.2015.1059644.

https://www.dropbox.com/sh/r8yfxwl7h602au6/AABGaKvMbEg7AnmijmTOApda?dl=0&preview=S079+-+Into+the+Great+Wide+Open+(1).pptx.


https://doi.org/10.5860/jifp.v2i1.6252.


**AASL Resources**

ALA Resources


California Law Resources


https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=6254.&lawCode=GOV.

https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=6267.&lawCode=GOV.

https://www.library.ca.gov/services/to-libraries/library-laws/.


https://adexchanger.com/privacy/california-gov-newsom-signs-7-ccpa-bills-into-law/.

RFP and Contract Resources and Templates


https://forallschools.s3.amazonaws.com/static/images/forallrubrics-
Negotiation Resources


Examples

Contract Addendums


Request For Proposals (from the RFP exercise)


New York City Department of Education. 2014. “RFP Information Security Requirements.”


SUNY. 2017. “Request for Proposal #CM03130 Library Services Platform.”

Vendor Assessment Tools


https://drive.google.com/drive/folders/1jdPwQeC5RAUbWLAhylYxWHa0pTdVObc