Policy Development

Protection of Personal Information of Library Users

COLORADO
Department of Education
Colorado State Library

FACT SHEET

Breaches of personal information are on the rise. The Colorado State Library sometimes receives questions about how libraries, as public facilities, should handle the protection of personal information of library users. It is recommended for libraries to have policies and procedures in place that clearly outline the library's responsibility and planned course of action for security practices and notifications of a security breach, should one occur. Parameters are set forth in the Colorado statutes, some of which are summarized here, along with best practices. This Fact sheet is provided for informational purposes, and is not intended as legal advice.

Definition of Personal Information

C.R.S. section 24-73-103 defines the term *personal information* as a combination of personal data elements that could compromise the security, confidentiality, or integrity of the individual in the event of a security breach. A *security breach* is defined as the unauthorized access of unencrypted personal information data.

Personal information is defined more clearly to be one of the following specific combinations of data:

- First name/initial, last name, and unencrypted *personal identifying information* (defined in C.R.S. 24-73-101) such as social security number, driver's license or state issued ID number, student or military ID number, or passport number;
- Username or email address, in combination with a password, PIN, or security questions and answers that would provide access to an online account;
- Account number or credit card/debit card number, in combination with any required security code, PIN number, access code, or password that would provide access to that account.

Personal identifying information is a more specific class of data, outlined in C.R.S. 24-73-101, and is limited to individual pieces of data that are highly sensitive. This means a social security number; personal identification number; password; passcode; official state or government issued driver's license or identification card number; government passport number; biometric data; employer, student, or military identification number; or financial transaction device.

Personal information differs from information that professional library values deems confidential, such as library user records and circulation data. Privacy of user records is covered in C.R.S. section 24-90-119.

For libraries that are not "governmental entities," see C.R.S. 6-1-713, 6-1-713.5, and 6-1-716 for the corresponding law that applies to all other business entities in the State of Colorado.

In the context of this Fact Sheet, the use of the words *personal information*, *personal identifying information*, and *security breach* reflects language from the statutes as cited. Refer to the statutes for more detailed definitions.

Best Practices

- Consult with local legal advisors on standard practices and legal requirements.
- Evaluate your library's current data storage policies and procedures to understand what data are collected, how they are stored and secured, and the time frame and methods for disposal.
- Implement a policy addressing disposal of library user data that contains personal information.
- Ensure that your library is implementing reasonable privacy and security practices to protect personal information. This includes agreements with third-party vendors.
- Have a plan to investigate if personal information was actually compromised in the event that a breach may occur.
- Implement a process to notify library patrons if a security breach has occurred, in accordance with state and federal laws.

Disposal Policy

C.R.S. section 24-73-101 states that each governmental entity must develop a written policy for the destruction and proper disposal of paper and electronic documents containing *personal identifying information*, once that information is no longer needed. It describes the manner of destruction and disposal to be done by "shredding, erasing, or otherwise modifying the *personal identifying information*" to make it unreadable or indecipherable through any means.

So, what does this mean for Colorado's city and county libraries and library districts? Depending on the governance structure, a city or county government may adopt a data disposal policy that covers all departments including the library. Library districts are defined as "political subdivisions of the State" and, therefore, generally will need to develop and adopt their own policy for data disposal. This policy may be included as part of a larger policy on information security, or it may be a stand-alone policy statement.

Sample policy language provided by various library jurisdictions may be found at:
http://www.cde.state.co.us/cdelib/librarydevelopment/publiclibraries/Policies.htm

Reasonable Security Practices

C.R.S. section 24-73-102 states that a governmental entity that maintains, owns, or licenses *personal identifying information* must implement "reasonable security procedures and practices" appropriate to the nature of the information. These procedures and practices could include storing paper documents containing such information in a secure area such as a locked room or locking file cabinet. Reasonable security procedures and practices for electronic information could include having secure web forms, storing *personal identifying information* using encryption (as opposed to plain text), and limiting access to such information to staff with a certain level of authority. In addition to the *personal identifying information* that the entity maintains or owns in its own buildings and servers, entities must provide for reasonable security practices with third party vendors. This means that governmental entities need to clearly outline in contracts with third party vendors the specific reasonable security practices that are required, as well as agreements for what third party vendors need to do in the event of a security breach.

So, what does this mean for Colorado's libraries? Libraries should begin by conducting an audit of what *personal identifying information* is stored by the library, where it is stored, and how it is being secured. For most if current security practices are not "reasonable" then the library should identify and implement improvements. Libraries also need to consider training for library staff who come into contact with *personal identifying information.* Staff training should include information on how to follow the libraries security practices, as well as provide context and explanation for the importance of this level of data protection. Libraries may also want to consider how much *personal identifying information* is collected from library users, and whether that information needs to be collected and stored. For example, some libraries may want to see a user's government-issued ID in order to establish residency, but it may not be necessary to collect, document, or store the actual ID number.

Notification of a Security Breach

C.R.S. section 24-73-103 states that government entities provide proper notice to law enforcement and individuals when a security breach of any *personal information* (as outlined in statute) occurs. It is important to first investigate a potential breach to confirm that personal information was actually compromised. Statute outlines the specifics of when, how, and to whom notification must be sent. Statute provides guidelines for what to include in the message regarding the data which has been compromised in the breach and advice to the individual to change their passwords, personal identification numbers, and security questions to secure their accounts. If a security breach occurs with a third-party vendor, it is the responsibility of the government entity to notify the individuals who are affected. If a security breach of *personal information* affects more than 500 Colorado residents, then the entity must notify the Colorado attorney general. If the security breach of *personal information* affects more than 1,000 Colorado residents, then the entity must also notify consumer credit reporting agencies, pursuant to the "Fair Credit Reporting Act."

So, what does this mean for Colorado's libraries? Libraries should have a procedural plan in place, to follow in the event of a security breach. This procedural plan should include details for how the library will investigate the level of threat from the security breach, notify and cooperate with law enforcement, notify affected library users, and notify other agencies as required by law. Failure to cooperate with this section of statute may bring action from the attorney general in order to force compliance.

Summary

To summarize, libraries should consider the following when looking at policies and procedures related to the protection of library user personal information data:

(1) Libraries should develop a policy for data disposal, unless they are already covered by the policy statement of their city or county government. This may be included as part of a larger policy on information security, or it may be a stand-alone policy statement.
(2) Libraries should conduct an audit of what *personal identifying information* is stored by the library, where it is stored, and how it is being secured. Libraries should also outline "reasonable security practices" for the protection of *personal identifying information.*
(3) Libraries should have a procedural plan in place to follow in the event of a potential security breach, which includes determining if a breach has in fact occurred. Libraries will need to consider what resources are available.
(4) This law also impacts the protection of personal information of staff, volunteers, and donors. It is important to consider these audiences as well when crafting policies and procedures for human resources, volunteer management, and donor management.
(5) For libraries that are not "governmental entities" see C.R.S. 6-1-713, 6-1-713.5, and 6-1-716 for the corresponding law that applies to all other business entities in the State of Colorado.
(6) Libraries should consult with legal advisors on the best approach to streamline this guidance so it provides helpful tips in your individual situation.

Additional Resources

- New Colorado Consumer Data Privacy Law Impacts Governmental Entities (Spencer Fane LLP) https://www.spencerfane.com/publication/new-colorado-consumer-data-privacy-law-impacts-governmental-entities/
- Library Laws, Policies, and Standards (Colorado State Library) http://www.cde.state.co.us/cdelib/librarydevelopment/publiclibraries/index
- Privacy Toolkit (American Library Association) http://www.ala.org/advocacy/privacy/toolkit