

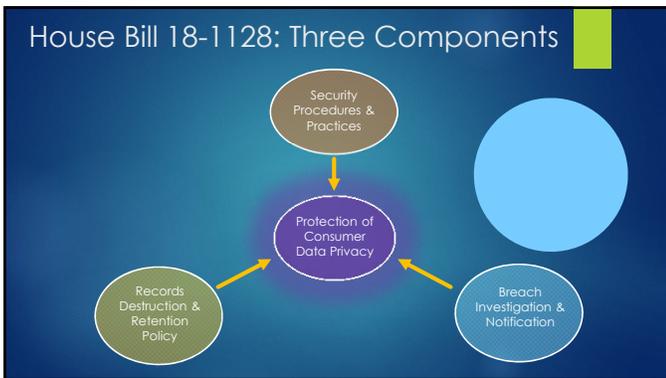
Colorado Protections for Consumer Data Privacy

HOUSE BILL 18-1128

The views expressed herein are solely those of the authors, and do not necessarily reflect the views of the Colorado Bar Association, the Greeley City Attorney's Office, or the City of Greeley U.T. Department. This presentation does not constitute legal advice. Speak with your own attorney and U.T. consultant before making any decisions.

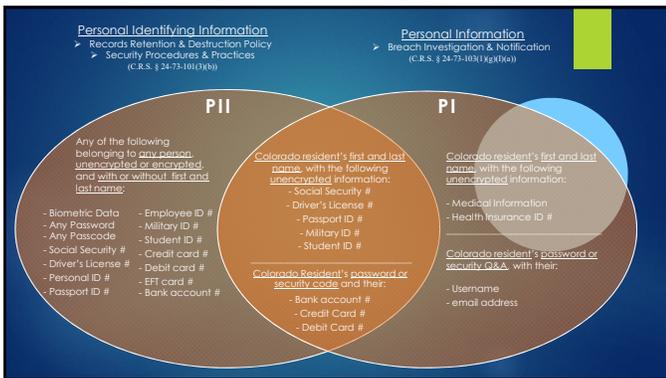
House Bill 18-1128

- ▶ H.B 18-1128 Signed into law on 29 May 2018
- ▶ Took effect 1 September 2018
- ▶ New definition of Personal Identifiable Information ("PII") and Personal Information ("PI")
- ▶ A "governmental entity" includes judicial departments, county, city and county, incorporated city or town, school district, special improvement district, authority and other district of the state organized pursuant to law.
- ▶ A "third-party service provider" is anyone who has been contracted to maintain, store, or process PII on behalf of a covered entity.



What is Personal Information ("PI") & Personal Identifying Information ("PII")?

- ▶ Social Security Number
- ▶ Personal identification number
- ▶ Password or Passcode
- ▶ Security Question and Answer
- ▶ Driver's license number or ID card number
- ▶ Passport number
- ▶ Biometric data
- ▶ Credit/Debit Card Number
- ▶ Security Code on back of card
- ▶ Employer, student, or military identification number
- ▶ Financial transaction device
- ▶ Username or email address
- ▶ Passwords or security questions/answers
- ▶ Account, credit, or debit numbers
- ▶ Security or access code
- ▶ Medical Information



House Bill 18-1128

RECORDS DESTRUCTION/RETENTION POLICY:

- ▶ "Each governmental entity . . . that maintains paper or electronic documents, . . . that contain personal identifying information shall develop a written policy for the destruction or proper disposal of those . . . documents." C.R.S. § 24-73-101(1)
- ▶ "Unless otherwise required by state or federal law, the written policy must require that, when such paper or electronic documents are no longer needed, the governmental entity destroy or arrange for the destruction of paper and electronic documents . . ." C.R.S. § 24-73-101(1)
- ▶ "A governmental entity that is regulated by state or federal law and that maintains procedures for disposal of personal identifying information pursuant to the laws, rules, regulations, guidances, or guidelines established by its state or federal regulator is in compliance with this section." C.R.S. § 24-73-101(2).

House Bill 18-1128

RECORDS DESTRUCTION/RETENTION POLICY:

House Bill 18-1128

SECURITY BREACH INVESTIGATION:

- Security Breach – "unauthorized acquisition of unencrypted computer data that compromises the security, confidentiality, or integrity of personal information maintained by a governmental entity." C.R.S. § 24-73-103(1)(h)
- Investigation and notification requirements also apply when encrypted personal information is breached, where the encryption key is also acquired. See C.R.S. § 24-73-103(2)(d).

House Bill 18-1128

SECURITY BREACH INVESTIGATION:

- "A governmental entity that maintains, owns, or licenses computerized data that includes personal information about a resident of Colorado shall, when it becomes aware that a security breach may have occurred, conduct in good faith a prompt investigation to determine the likelihood that personal information has been or will be misused." C.R.S. § 24-73-103(2).
- "The governmental entity shall give notice to the affected Colorado residents unless the investigation determines that the misuse of information about a Colorado resident has not occurred and is not reasonably likely to occur." C.R.S. § 24-73-103(2).

House Bill 18-1128

SECURITY BREACH NOTIFICATION :

- Unless the investigation determines the breach has not and will not likely lead to misuse of PII, the governmental entity must send notice of the breach to the affected Colorado residents within 30 days, including:
 - Date
 - description of PI involved;
 - governmental entity's contact information;
 - consumer reporting agencies - toll-free phone number, address, and website (e.g. Equifax, TransUnion);
 - Federal Trade Commission - toll-free phone number, address, and website;
 - statement that resident can obtain fraud alerts and security freezes; and
 - directions to change passwords and security questions, if the type of PI breached was a password or security Q&A, in combination with a username or email address
- See C.R.S. § 24-73-103(2)(a)-(c).

House Bill 18-1128

SECURITY BREACH NOTIFICATION :

- If the breach affects more than 500 Colorado residents, then the governmental entity must also notify the Colorado Attorney General's Office within 30 days
- If the breach affects more than 1,000 Colorado residents, then the governmental entity must also notify all consumer reporting agencies of the date notice was sent to the residents and the number of residents notified.
- Vendor's Cooperation in Reporting Breaches:
 - Third-party service providers are required to cooperate with government entity's breach investigation and notification requirements:
 - Promptly notify the governmental entity of a breach
 - Inform the governmental entity if misuse of the PI has occurred or is likely to occur
 - Provide all information relevant to the breach

House Bill 18-1128

Security Procedures – Government Entities

- Requires governmental entities that maintain, own, or license PII to implement and maintain reasonable security procedures that are appropriate to the type of PII dealt with and the size of the government entity. See C.R.S. § 24-73-102(1).
 - Applies to governmental entities who maintain, own or license PII, *id.*
 - Must be designed to prevent against unauthorized access, use, modification, disclosure, or destruction, *id.*
- Keep in mind, the definition of PII does not require electronic format; applies to paper documents, ID badges, etc.

House Bill 18-1128

▶ Security Procedures – Government Entities' Vendors

- ▶ "Unless a governmental entity agrees to provide its own security protection for the information it discloses to a third-party service provider, the governmental entity shall require that the third-party service provider implement and maintain reasonable security procedures and practices that are:
 - ▶ Appropriate to the nature of the personal identifying information disclosed to the third-party service provider; and
 - ▶ Reasonably designed to help protect the personal identifying information from unauthorized access, use, modification, disclosure, or destruction." C.R.S. § 24-73-102(2)



What Does This Mean to Local Governments in Colorado?

- ▶ Implement appropriate security procedures to protect PII.
- ▶ Make sure that our vendors who handle PII have appropriate security procedures in place and are required to notify you of data breaches and assist you with remediation.
- ▶ Maintain a written policy for document (hardcopy and digital) destruction when PII is no longer needed.
- ▶ Implement a data breach notification policy with notice provided to individuals no later than 30 days after determination that a breach occurred. The notification requires significant detail and additional notification to the Colorado Attorney General's office and credit reporting agencies if certain thresholds are met.



Protection of PII

- ▶ Adopting industry best practices (NIST or ISO)
- ▶ Do your vendors conduct SOC2 or SOC3 audits?
- ▶ Can you access results?
- ▶ NIST SP800-122 and NIST SP800-53 to safeguard PII
- ▶ Standards include
 - ▶ Access and retention rules
 - ▶ Incident response and data breach notification
 - ▶ Limitation of collection, disclosure, sharing and use of PII
 - ▶ Data loss prevention
 - ▶ Media safe handling
 - ▶ Protection of data at rest and in transit



Mitigation Steps

NIST SP 800-122 Guide to Protecting PII

- ▶ **Operational Safeguards**
 - ▶ Perform assessment to discover where PII is stored and how it's processed
 - ▶ Data Security Categorization
 - ▶ Breach Notification Policy
 - ▶ Update/Amend Access Controls
 - ▶ Media Protection Policy
 - ▶ Periodic review of who can access PII
- ▶ **Strategic Safeguards**
 - ▶ Minimize the use, collection, and retention of PII
 - ▶ Data encryption at rest and in transit
 - ▶ Media protection: storage, marking, transport, and sanitization
 - ▶ Secure e-mail containing PII
 - ▶ Secure physical storage of hardcopy documents
 - ▶ Access control to sensitive storage through prox cards, cipher locks or keys



Additional Common Safeguards

- ▶ Access Enforcement
- ▶ Separation of Duties
- ▶ Least Privilege
- ▶ Remote Access (limit/restrict)
- ▶ Collaboration/Information Sharing
- ▶ Mobile Device Access Control
- ▶ Event Logging
- ▶ Audit Reviews
- ▶ Two Factor Authentication
- ▶ Media Access
- ▶ Media Marking
- ▶ Media Storage
- ▶ Media Transport
- ▶ Media Sanitization
- ▶ Secure E-mail
- ▶ Data Loss Prevention
- ▶ Protection at Rest
- ▶ System Monitoring



<p>Jeremy Schupbach <i>Director Of Legislative Relations</i> Colorado Bar Association 1290 Broadway 1700 Denver, Colorado 80203 (303) 824-5309 jschupbach@cobar.org</p>	<p>Aaron Goldman <i>Environmental and Water Resources Attorney</i> Greeley City Attorney's Office 1100 10th Street, Suite 401 Greeley, Colorado 80631 (970) 350-9819 Aaron.Goldman@Greeleygov.com</p>	<p>Jay Britt <i>Security Analyst</i> Greeley Information Technology 1001 11th Ave., Ste. 300 Greeley, Colorado 80631 (970) 350-9887 Jay.Britt@Greeleygov.com</p>
--	--	---

