Using Data to Improve Education: A Legal Reference Guide to Protecting Student Privacy and Data Security

State Security Breach Response Laws

State-by-State Summary Table

Last Updated: February 2011.

As state policymakers implement statewide longitudinal data systems that collect, store, link and share student-level data, it is critical that they understand applicable privacy and data security standards and laws designed to ensure the privacy, security and confidentiality of that data. To help state policymakers navigate this complex legal landscape, the Data Quality Campaign has partnered with Education Counsel and the Information Management Practice of Nelson Mullins Riley & Scarborough to develop *Using Data to Improve Education: A Legal Reference Guide to Protecting Student Privacy and Data Security*. This guide provides summaries of multiple federal and state laws that have implications for statewide longitudinal data systems. The full guide can be accessed in multiple ways: by federal law, state law by issue and state law by state. Visit www.dataqualitycampaign.org/privacy_guide.

The information provided here is intended to serve as a good starting place for policymakers. For more detailed information about any of the specific state laws, please contact Jon A. Neiditz, Partner, Nelson Mullins Riley & Scarborough LLP at jon.neiditz@nelsonmullins.com or 404.322.6139.

State, Law & Effective Date	Triggering Event (Risk / Harm or Access)	Electronic Only or Paper Included?	"Personal Information" Definition As Compared To CA Definition*	Exception for Encryption or Redaction?	Applicable to State or Government Agencies?[1]	Pre-Breach Measures Included in Breach Law?	Timing of Notification Following Determination of Scope Of Breach & Restoration Of System Integrity	Civil or Criminal Penalties?	Private Right of Action Included in Breach Law?	Criminal Investigation or Publicly Available Information Exception?	Other Parties to be Notified? (Excludes State Agency Obligations)
Alabama											
Alaska Alaska Stat. § 45.48.010 et seq. 6/14/08	Unauthorized acquisition, or reasonable belief of unauthorized acquisition, that compromises security, confidentiality or integrity of Personal Information ("PI") unless *no reasonable likelihood of harm* (must retain documentation for 5 years); "acquisition" defined	Paper & electronic	Modified CA – account number, credit card or debit card number alone unless can only be accessed with a personal code; also passwords, PINs or access codes for financial accounts	Encryption (unless encryption key is also disclosed) or redaction	Yes, applies to governmental agencies.	Yes, provisions relating to use, display and communication of Social Security numbers, provisions relating to destruction and disposal of paper documents with PI and implementation of policies and procedures relating to destruction of electronic media (effective 7/1/09)	Most expedient manner possible and without unreasonable delay unless after reasonable investigation and written notice to Attorney General determine *no reasonable likelihood of harm* (must retain documentation for 5 years)	Yes	Only for breach of pre-breach measures relating to disposal of records	Yes, both	Attorney General if no notification provided; Consumer Reporting Agencies if notifying 1,000+ AK residents unless subject to GLBA

[1] This analysis assumes that a law that states it applies to "a person who conducts business in this state" without specifically defining person to include state or governmental agencies does not apply to such agencies.

*"CA" = California's initial definition of "Personal Information," which was "an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (1) Social security number, (2) Driver's license number or California Identification Card number (3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account." Ca. Civ. Code § 1798.82(e).

State, Law & Effective Date	Triggering Event (Risk / Harm or Access)	Electronic Only or Paper Included?	"Personal Information" Definition As Compared To CA Definition*	Exception for Encryption or Redaction?	Applicable to State or Government Agencies?[1]	Pre-Breach Measures Included in Breach Law?	Timing of Notification Following Determination of Scope Of Breach & Restoration Of System Integrity	Civil or Criminal Penalties?	Private Right of Action Included in Breach Law?	Criminal Investigation or Publicly Available Information Exception?	Other Parties to be Notified? (Excludes State Agency Obligations)
Arkansas Ark. Code § 4-110-101 et seq. 3/31/05	Unauthorized acquisition of computerized data that compromises security, confidentiality or integrity of PI unless no reasonable likelihood of *harm*	Electronic	CA plus medical information if not encrypted or redacted	Encryption or redaction	No	Yes, security procedures and all reasonable steps to destroy by shredding, erasing or otherwise modifying PI to make unreadable or undecipherable	Following discovery or notification of breach and most expedient time and manner possible and without unreasonable delay unless no reasonable likelihood of harm	Yes	No	Yes, both	No
California Cal. Civ. Code § 1798.80 et seq. & 1798.29 (gov't agencies) 7/1/03 & 1/1/07	Unauthorized acquisition of computerized data that compromises security, confidentiality or integrity of PI	Electronic	CA plus medical & health insurance information (revised)	Encryption	Yes	Yes, all reasonable steps to destroy by shredding, erasing or otherwise modifying PI to make unreadable. Also, reasonable security procedures.	Following discovery or notification of breach and most expedient time and manner possible and without unreasonable delay	No	Yes	Yes, both	No
Colorado Col. Rev. Stat. § 6-1-716 9/1/06 6-1-713 8/4/2004	Unauthorized acquisition of computerized data that compromises security, confidentiality or integrity of PI unless investigation finds misuse of PI has not occurred or will not reasonably likely occur	Electronic	CA plus redacted or secured by other method to make unreadable or unusable	Encryption, redaction or secured by other method to make unreadable or unusable	If entity subject to guidelines of primary or functional state or federal regulator	Each public and private entity in the state that uses documents during the course of business that contain personal identifying information shall develop a policy for the destruction or proper disposal of paper documents containing personal identifying information. "Personal identifying information" means a SSN, personal ID #, password, pass code, an official state or gov't issued driver's license or ID #, a gov't passport #, biometric data, an employer, student or military ID # or a financial transaction device. Public entities managing records in part 1 of Art. 80 of title 24 of the Colo. Rev. States shall be deemed to have complied with this provision.	Most expedient time and manner possible and without unreasonable delay unless investigation finds misuse of PI has not occurred or will not reasonably likely occur	Yes	No	Yes, both	Consumer Reporting Agencies if notifying 1,000+ CO residents unless subject to GLBA

*"CA" = California's initial definition of "Personal Information," which was "an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (1) Social security number, (2) Driver's license number or California Identification Card number (3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account." Ca. Civ. Code § 1798.82(e).

State, Law & Effective Date	Triggering Event (Risk / Harm or Access)	Electronic Only or Paper Included?	"Personal Information" Definition As Compared To CA Definition*	Exception for Encryption or Redaction?	Applicable to State or Government Agencies?[1]	Pre-Breach Measures Included in Breach Law?	Timing of Notification Following Determination of Scope Of Breach & Restoration Of System Integrity	Civil or Criminal Penalties?	Private Right of Action Included in Breach Law?	Criminal Investigation or Publicly Available Information Exception?	Other Parties to be Notified? (Excludes State Agency Obligations)
Connecticut Conn. Gen. Stat. 36A-701(b) 1/1/06 Conn. Gen. Stat. § 42-471 10/1/08	Unauthorized access to or acquisition of electronic files, media, databases or computerized data; no breach if, after an appropriate investigation and consultation with relevant federal, state and local agencies responsible for law enforcement, reasonably determine that ***harm*** will not likely result from breach.	Electronic	CA	Encryption or secured by other method to make unreadable or unusable	No	(effective 10/1/08) If possess PI, must safeguard the data, computer files and documents with PI from misuse by third parties, and destroy, erase or make unreadable such data, computer files and documents prior to disposal; also must publicly display privacy protection policy if collect Social Security numbers	Without unreasonable delay unless if, after an appropriate investigation and consultation with relevant federal, state and local agencies responsible for law enforcement, the person reasonably determines that harm will not likely result from breach	Yes	No	Yes, both	No
Delaware De. Code tit. 6, § 12B-101 et seq. 6/28/05	Unauthorized acquisition of computerized data that compromises security, confidentiality or integrity of PI unless investigation finds ***misuse*** of PI has not occurred or will not reasonably likely occur	Electronic	CA	Encryption	Yes, applies to governments, governmental subdivisions, agencies, and instrumentalities.	No	Most expedient time and manner possible and without unreasonable delay unless investigation finds misuse of PI has not occurred or will not reasonably likely occur.	Yes	No	Yes, both	No
Florida Fla. Stat. § 817.5681 7/1/05	Unlawful & unauthorized acquisition of computerized data that ***materially*** compromises security, confidentiality or integrity of PI unless investigation finds ***misuse*** of PI has not occurred or will not reasonably likely occur (must retain documentation for 5 years)	Electronic	CA	Encryption	Yes, applies to gov't agencies or subdivisions except that fines do not apply to gov't entities, but third party engaged by such entity to perform gov't services would be liable for such fines.	No	Without unreasonable delay, but ***no later than 45 days*** unless investigation finds misuse of PI has not occurred or will not reasonably likely occur (must retain documentation for 5 years)	Yes (gov't agencies exempt from fines)	No	Yes, both	Consumer Reporting Agencies if notifying 1,000+ FL residents

*"CA" = California's initial definition of "Personal Information," which was "an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (1) Social security number, (2) Driver's license number or California Identification Card number (3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account." Ca. Civ. Code § 1798.82(e).

State, Law & Effective Date	Triggering Event (Risk / Harm or Access)	Electronic Only or Paper Included?	"Personal Information" Definition As Compared To CA Definition*	Exception for Encryption or Redaction?	Applicable to State or Government Agencies?[1]	Pre-Breach Measures Included in Breach Law?	Timing of Notification Following Determination of Scope Of Breach & Restoration Of System Integrity	Civil or Criminal Penalties?	Private Right of Action Included in Breach Law?	Criminal Investigation or Publicly Available Information Exception?	Other Parties to be Notified? (Excludes State Agency Obligations)
Georgia Ga. Code § 10-1-910 et seq. 5/5/05 *(Applies only to "information brokers" and governmental agencies)*	Unauthorized acquisition of computerized data maintained by an information broker or governmental data collector that compromises security, confidentiality or integrity of PI	Electronic	Modified CA – account number, credit card or debit card number alone unless can only be accessed with additional info; also passwords, personal ID #s or access codes; plus information sufficient to perform or attempt to perform identity theft	Encryption or redaction	Yes, applies to any state or local agency or subdivision thereof including any dept., bureau, authority, public university or college, academy, commission, or other gov't entity[2]	Ga. Code § 10-15-2, eff. 2002, A business may not discard a record containing PI[3] unless (1) shred customer's record before discarding; (2) erase the PI contained in the customer's record before discarding the record; (3) modify customer's record to make the PI unreadable before discarding; or (4) take actions that it reasonably believes will ensure that no unauthorized person will have access to PI contained in customer's record for the period between the record's disposal and the record's destruction	Most expedient time and manner possible and without unreasonable delay	No	No	Yes, both	Consumer Reporting Agencies if notifying 10,000+ GA residents
Hawaii Hawaii Rev. Stat. § 487N-2 1/1/07 Haw. Rev. Stat. § 487R-2 4/17/2008	Unauthorized access to and acquisition of records or data where *illegal use* has occurred, is reasonably likely to occur and creates risk of harm	Any form	CA	Encryption or redaction (unless confidential process or key is also disclosed)	Yes, applies to gov't agencies, which include any department, division, board, commission, public corporation, or other agency or instrumentality of the State or of any county.	Yes, extensive disposal measures required in Haw. Stat. § 487R-2, but excludes entities subject to GLBA, HIPAA or FCRA	Following discovery or notification and without unreasonable delay	Yes (but government agencies exempt)	Yes (but not against government agencies)	Yes, both	If notifying 1,000+ HI residents, Hawaii Office of Consumer Protection and Consumer Reporting Agencies

[2] Georgia's security breach law does not apply to any governmental agency whose records are maintained primarily for traffic safety, law enforcement, or licensing purposes or for purposes of providing public access to court records or to real or personal property information.

[3] Ga. Code §10-15-1(9). "Personal information" means: (A) Personally identifiable data about a customer's medical condition, if the data are not generally considered to be public knowledge; (B) Personally identifiable data which contain a customer's account or identification number, account balance, balance owing, credit balance, or credit limit, if the data relate to a customer's account or transaction with a business;(C) Personally identifiable data provided by a customer to a business upon opening an account or applying for a loan or credit; or (D) Personally identifiable data about a customer's federal, state, or local income tax return. (10)(A) "Personally identifiable" means capable of being associated with a particular customer through one or more identifiers, including, but not limited to, a customer's fingerprint, photograph, or computerized image, social security number, passport number, driver identification number, personal identification card number, date of birth, medical information, or disability information. (B) A customer's name, address, and telephone number shall not be considered personally identifiable data unless one or more of them are used in conjunction with one or more of the identifiers listed in subparagraph (A) of this paragraph.

*"CA" = California's initial definition of "Personal Information," which was "an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (1) Social security number, (2) Driver's license number or California Identification Card number (3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account." Ca. Civ. Code § 1798.82(e).

State, Law & Effective Date	Triggering Event (Risk / Harm or Access)	Electronic Only or Paper Included?	"Personal Information" Definition As Compared To CA Definition*	Exception for Encryption or Redaction?	Applicable to State or Government Agencies?[1]	Pre-Breach Measures Included in Breach Law?	Timing of Notification Following Determination of Scope Of Breach & Restoration Of System Integrity	Civil or Criminal Penalties?	Private Right of Action Included in Breach Law?	Criminal Investigation or Publicly Available Information Exception?	Other Parties to be Notified? (Excludes State Agency Obligations)
Idaho Id. Code §§ 28-51-104 to 28-51-107 7/1/06, H.B. 566, amending § 28-51-05, eff. 3/31/10	Illegal acquisition of computerized data that *materially* compromises security, confidentiality or integrity of PI unless investigation finds *misuse* of PI has not occurred or will not reasonably likely occur	Electronic	CA	Encryption	Yes, applies to state and local agencies.	No	Most expedient time possible and without unreasonable delay unless investigation finds misuse of PI has not occurred or will not reasonably likely occur	Yes	No	Yes, both	*Eff. 3/31/10*, state agencies must notify AG within 24 hours of discovery of breach; must also notify chief information officer of dept. of administration
Illinois 815 Ill. Comp. Stat. 530/1 et seq. 1/1/06 20 Ill. Comp. Stat. 450/ 1 et seq., 7/23/03	Unauthorized acquisition of computerized data that compromises security, confidentiality or integrity of PI	Electronic	CA	Encryption or redaction	Yes, applies to government agencies, public and private universities	Yes, extensive disposal procedures required for data stored on State-owned electronic data processing equipment. Applies to the Department of Central Mgt Services or an authorized agency (other than public universities or their governing boards). However, the governing board of each public university must implement and administer the provisions of this Act with respect to State-owned electronic data processing equipment utilized by the university.	Most expedient time possible and without unreasonable delay	Violation constitutes unlawful practice under Consumer Fraud and Deceptive Business Practices Act	Yes	Yes, both	No

*"CA" = California's initial definition of "Personal Information," which was "an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (1) Social security number, (2) Driver's license number or California Identification Card number (3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account." Ca. Civ. Code § 1798.82(e).

State, Law & Effective Date	Triggering Event (Risk / Harm or Access)	Electronic Only or Paper Included?	"Personal Information" Definition As Compared To CA Definition*	Exception for Encryption or Redaction?	Applicable to State or Government Agencies?[1]	Pre-Breach Measures Included in Breach Law?	Timing of Notification Following Determination of Scope Of Breach & Restoration Of System Integrity	Civil or Criminal Penalties?	Private Right of Action Included in Breach Law?	Criminal Investigation or Publicly Available Information Exception?	Other Parties to be Notified? (Excludes State Agency Obligations)
Indiana Ind. Code § 24-4.9 Ind. Code § 24-4-14 7/1/06	Unauthorized acquisition of computerized data that compromises security, confidentiality or integrity of PI if the unauthorized acquisition has resulted in or could result in *identity deception* (as defined in IC 35-43-5-3.5), identity theft, or fraud affecting the IN resident	Electronic and non-computerized	CA + *financial* account number, etc. instead of account number, etc.	Encryption or redaction (unless confidential process or key is also disclosed)	Yes, applies to state and local agencies	Yes, when disposing of unencrypted, unredacted PI, must shred, incinerate, mutilate, erase, or otherwise render PI illegible or unusable – failing to is Class C infraction, if for 100+ customers = Class A infraction (exempts certain gov't agencies and those subject to FCRA, HIPAA, Patriot Act, Financial Modern. Act & Exec Order. 13224)	Without unreasonable delay if the unauthorized acquisition has resulted in or could result in identity deception (as defined in IC 35-43-5-3.5), identity theft, or fraud affecting the IN resident	Yes	No	Yes, both	Consumer Reporting Agencies if notifying 1,000+ IN residents
Iowa Iowa Code §§ 715C.1 & 715C.2 7/1/08	Unauthorized acquisition of PI maintained in computerized form that compromises security, confidentiality or integrity of PI unless determine no reasonable likelihood of ***financial harm*** (maintain documentation for 5 years)	Computerized	CA + ***financial*** account number, etc. instead of account number, etc., unique electronic identifier or routing code with access code permitting access or unique biometric data	Encryption, redaction or altered by any method or technology so name or data elements are unreadable	Yes, applies to government, gov't subdivision, agency, or instrumentality.	No	Most expeditious manner possible & without unreasonable delay unless determine no reasonable likelihood of financial harm (maintain documentation for 5 years)	Yes, unlawful practice pursuant to § 714.16 (Consumer FraulOds)	No	Yes, both	No

*"CA" = California's initial definition of "Personal Information," which was "an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (1) Social security number, (2) Driver's license number or California Identification Card number (3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account." Ca. Civ. Code § 1798.82(e).

State, Law & Effective Date	Triggering Event (Risk / Harm or Access)	Electronic Only or Paper Included?	"Personal Information" Definition As Compared To CA Definition*	Exception for Encryption or Redaction?	Applicable to State or Government Agencies?[1]	Pre-Breach Measures Included in Breach Law?	Timing of Notification Following Determination of Scope Of Breach & Restoration Of System Integrity	Civil or Criminal Penalties?	Private Right of Action Included in Breach Law?	Criminal Investigation or Publicly Available Information Exception?	Other Parties to be Notified? (Excludes State Agency Obligations)
Kansas Kansas Stat. 50-7a01, 50-7a02, 50-7a03 7/1/06	Unauthorized access to and acquisition of computerized data that compromises security, confidentiality or integrity of PI and causes or is reasonably believed to cause ***ID theft*** to a consumer	Electronic	CA+ ***financial*** account number, credit or debit card number, ***alone*** or in combination with any required security code, access code or password that would permit access to a consumer's financial account.	Encryption or redaction	Yes, applies to government or governmental subdivision or agency.	Yes, all reasonable steps to destroy by shredding, erasing or otherwise modifying PI to make unreadable	Most expedient time possible and without unreasonable delay unless investigation finds misuse of PI has not occurred or will not reasonably likely occur	Yes	No	Yes, both	Consumer Reporting Agencies if notifying 1,000+ Kan. residents
Kentucky											
Louisiana La. Rev. Stat. § 51:3071 et seq. 1/1/06	Compromise of security, confidentiality or integrity of computerized data that results in, or reasonably could result in, unauthorized acquisition of and access to PI unless reasonable investigation finds no reasonable likelihood of ***harm*** to customers	Electronic	CA plus redacted	Encryption or redaction	Yes, applies to a political subdivision of the state, and any officer, agency, board, commission, department or similar body of the state or any political subdivision of the state.	No	Most expedient time possible and without unreasonable delay unless reasonable investigation finds no reasonable likelihood of harm to customers	No	Yes	Yes, both	No

*"CA" = California's initial definition of "Personal Information," which was "an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (1) Social security number, (2) Driver's license number or California Identification Card number (3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account." Ca. Civ. Code § 1798.82(e).

State, Law & Effective Date	Triggering Event (Risk / Harm or Access)	Electronic Only or Paper Included?	"Personal Information" Definition As Compared To CA Definition*	Exception for Encryption or Redaction?	Applicable to State or Government Agencies?[1]	Pre-Breach Measures Included in Breach Law?	Timing of Notification Following Determination of Scope Of Breach & Restoration Of System Integrity	Civil or Criminal Penalties?	Private Right of Action Included in Breach Law?	Criminal Investigation or Publicly Available Information Exception?	Other Parties to be Notified? (Excludes State Agency Obligations)
Maine Me. Rev. Stat. tit. 10 §§ 1347 et seq. 1/31/06 (rev'd 1/31/07), amended by Public Law, Chap. 161 (eff. 9/12/09)	Unauthorized acquisition of computerized data that compromises security, confidentiality or integrity of PI unless reasonable & prompt investigation finds no ***misuse*** or reasonable likelihood of misuse of PI	Electronic	SSN, Driver's license or state ID #, account #, credit card # or debit card # if could be used w/o access code or password, password, PINs or any of the above if sufficient to permit ID theft	Encryption or redaction	Yes, applies to gov't agencies, the University of Maine System, the Maine Community College System, Maine Maritime Academy and private colleges and universities.	No	As expediently as possible and without unreasonable delay unless reasonable & prompt investigation finds no misuse or reasonable likelihood of misuse of PI; *eff. 9/12/09*, notice may not be delayed by more than *7 business days* after a law enforcement agency determines that notification will not compromise a criminal investigation.	Yes	No	Yes, both	Consumer Reporting Agencies if notifying 1,000+ persons. Either state regulator or attorney general if any notice made
Maryland Md. Code, Com. Law §§ 14-3501 – 14-3508 1/1/08	Unauthorized acquisition of computerized data that compromises security, confidentiality or integrity of PI unless reasonable & prompt investigation finds no misuse or reasonable likelihood of misuse of PI (must retain documentation for ***3 years***)	Electronic	CA, ***financial*** account #, etc. + an individual taxpayer identification number	Encryption, redaction or otherwise protected by another method that renders it unreadable or unusable	No	Reasonable steps to protect PI during destruction; maintain reasonable security procedures & practices; must contractually require 3rd party service providers to maintain reasonable security procedures & practices (3rd party contract requirement effective 1/1/09)	As soon as reasonably practicable unless reasonable & prompt investigation finds no misuse or reasonable likelihood of misuse of PI (must retain documentation for ***3 years*** if no notification provided)	Yes, unfair or deceptive trade practice under Title 13 of Article 14, subject to its enforcement and penalty provisions	Yes	Yes, both plus if individual consented to public dissemination or disseminated in accordance with HIPAA	Must notify Office of Attorney General prior to providing notification to individuals; if notifying 1,000+ persons, must notify consumer reporting agencies

*"CA" = California's initial definition of "Personal Information," which was "an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (1) Social security number, (2) Driver's license number or California Identification Card number (3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account." Ca. Civ. Code § 1798.82(e).

State, Law & Effective Date	Triggering Event (Risk / Harm or Access)	Electronic Only or Paper Included?	"Personal Information" Definition As Compared To CA Definition*	Exception for Encryption or Redaction?	Applicable to State or Government Agencies?[1]	Pre-Breach Measures Included in Breach Law?	Timing of Notification Following Determination of Scope Of Breach & Restoration Of System Integrity	Civil or Criminal Penalties?	Private Right of Action Included in Breach Law?	Criminal Investigation or Publicly Available Information Exception?	Other Parties to be Notified? (Excludes State Agency Obligations)
Massachusetts Mass. Gen. Laws ch. 93H, §1 et al 2/3/08 201 CMR 17.00 – 17.04 3/1/2010	Unauthorized acquisition of data or electronic data that compromises security, confidentiality or integrity of PI and creates a ***substantial risk of ID theft or fraud***	Electronic and any other material upon which written, drawn, spoken, visual or electromagnetic information or images are recorded	CA + financial account number, etc., but without encryption; also, with ***or without*** security code, access, code, PIN or password	Encryption (unless confidential process or key is also disclosed)	Yes, applies to any agency, executive office, department, board, commission, bureau, division or authority of the commonwealth, or any of its branches, or of any political subdivision thereof.	Yes, dispose of PI by redacting, shredding, pulverizing or burning to make unreadable or unable to be reconstructed (Mass. Gen. Laws. Ch. 93I, § 2); must develop, implement & maintain information security program consistent with industry standards that contains administrative, technical & physical safeguards to ensure security & confidentiality of records with PI (specific components of program described as well) (effective 3/1/10, 201 CMR 17.03); must implement computer system security requirements including encryption of all stored PI and all wireless transmissions of PI where technically feasible (effective 3/1/10, 201 CMR 17.04)	As soon as practicable and without unreasonable delay when know or have reason to know of breach or PI has been acquired or used by unauthorized person or used for an unauthorized purpose; must document responsive actions taken in connection with any incident involving a security breach, including any changes in business practices (effective 3/1/10, 201 CMR 17.03)	Yes	No	Yes, both	Attorney General, director of office of consumer affairs and business regulation and consumer reporting agencies identified by director
Michigan Mich. Comp. Laws, §445.61 et seq. 6/29/07	Unauthorized acquisition of or access to data that compromises security or confidentiality of PI maintained as part of a ***database*** of PI regarding multiple individuals; no breach if it has not or will not likely cause substantial loss or injury or result in identity theft	Electronic	CA+ demand deposit or other financial account number, etc. instead of account number	Encryption or redaction (unless confidential process or key is also disclosed)	Yes, applies to any department, board, commission, office, agency, authority, or other unit of state government and includes an institution of higher education.	Yes, destroying by shredding, erasing or otherwise modifying PI to make unreadable if no longer needed	Without unreasonable delay after discovery or notice unless breach has not or will not likely cause substantial loss or injury or result in identity theft	Yes	No	Yes, both	Consumer Reporting Agencies if notifying 1,000+ persons unless subject to GLBA

*"CA" = California's initial definition of "Personal Information," which was "an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (1) Social security number, (2) Driver's license number or California Identification Card number (3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account." Ca. Civ. Code § 1798.82(e).

State, Law & Effective Date	Triggering Event (Risk / Harm or Access)	Electronic Only or Paper Included?	"Personal Information" Definition As Compared To CA Definition*	Exception for Encryption or Redaction?	Applicable to State or Government Agencies?[1]	Pre-Breach Measures Included in Breach Law?	Timing of Notification Following Determination of Scope Of Breach & Restoration Of System Integrity	Civil or Criminal Penalties?	Private Right of Action Included in Breach Law?	Criminal Investigation or Publicly Available Information Exception?	Other Parties to be Notified? (Excludes State Agency Obligations)
Minnesota Minn. Stat. § 325E.61 1/1/06	Unauthorized acquisition of computerized data that compromises security, confidentiality or integrity of PI	Electronic	CA plus other method that makes data unreadable or unusable	Encryption or other method (unless key is also disclosed)	No	No	Most expedient time possible and without unreasonable delay	Yes	No	Yes, both	Consumer Reporting Agencies if notifying 500+ *within 48 hours*
Mississippi Miss. HB 583 7/1/2011	Unauthorized acquisition of electronic files, media, databases or computerized data. Notification ***not*** required if, after an appropriate investigation, reasonably determine that the breach ***will not likely result in harm*** to affected individuals	Electronic	CA	Encryption or secured by any other method or technology that renders the personal information unreadable or unusable	No	No	Without unreasonable delay, subject to law enforcement exception and completion of investigation to determine nature and scope of incident, to identify affected individuals, or to restore reasonable integrity of the data system. Notification *not* required if, after an appropriate investigation, reasonably determine that the breach *will not likely result in harm* to affected individuals.	Violation considered an unfair trade practice.	No	Yes, both	No

*"CA" = California's initial definition of "Personal Information," which was "an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (1) Social security number, (2) Driver's license number or California Identification Card number (3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account." Ca. Civ. Code § 1798.82(e).

State, Law & Effective Date	Triggering Event (Risk / Harm or Access)	Electronic Only or Paper Included?	"Personal Information" Definition As Compared To CA Definition*	Exception for Encryption or Redaction?	Applicable to State or Government Agencies?[1]	Pre-Breach Measures Included in Breach Law?	Timing of Notification Following Determination of Scope Of Breach & Restoration Of System Integrity	Civil or Criminal Penalties?	Private Right of Action Included in Breach Law?	Criminal Investigation or Publicly Available Information Exception?	Other Parties to be Notified? (Excludes State Agency Obligations)
Missouri Mo. Rev. Stat. § 407.1500 8/28/09	Unauthorized access to and unauthorized acquisition of PI maintained in computerized form that compromises the security, confidentiality, or integrity of the PI.	Electronic	CA + Unique electronic identifier or routing code, in combination with any required security code, access code, or password that would permit access to an individual's financial account; medical information[4] or health insurance information[5].	Encryption, redaction, or otherwise altered by any method or technology in such a manner that the name or data elements are unreadable or unusable	Yes, applies to government, governmental subdivision, governmental agency and governmental instrumentality	No	Made without unreasonable delay; notification ***not*** required if, after an appropriate investigation or after consultation with relevant federal, state, or local agencies, determine that a *risk of identity theft or other fraud* to any consumer is not reasonably likely to occur as a result of the breach. Such a determination shall be documented in writing and the documentation shall be *maintained for five years*.	Yes, civil	No	Yes, both	If notifying 1,000+ MO residents, notify, without unreasonable delay, the AG's office and all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis of the timing, distribution, and content of the notice.
Montana Mont. Code § 30-14-1701 et seq. 3/1/06	Unauthorized acquisition of computerized data that compromises security, confidentiality or integrity of PI and causes or is reasonably likely to cause loss or injury	Electronic	CA + tribal identification number	Encryption	No	Yes, all reasonable steps to destroy by shredding, erasing or otherwise modifying PI to make unreadable where PI defined as name, signature, address, or telephone number, in combination with one or more of following: passport number, driver's license or state ID #, insurance policy #, bank account #, credit card or debit card #, passwords or personal identification #s required to obtain access to the individual's finances, or any other financial information. SSN alone constitutes PI	Without unreasonable delay	Yes	No	Yes, both	No

[4] "Medical information", any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.
[5] "Health insurance information", an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual.
*"CA" = California's initial definition of "Personal Information," which was "an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (1) Social security number, (2) Driver's license number or California Identification Card number (3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account." Ca. Civ. Code § 1798.82(e).

State, Law & Effective Date	Triggering Event (Risk / Harm or Access)	Electronic Only or Paper Included?	"Personal Information" Definition As Compared To CA Definition*	Exception for Encryption or Redaction?	Applicable to State or Government Agencies?[1]	Pre-Breach Measures Included in Breach Law?	Timing of Notification Following Determination of Scope Of Breach & Restoration Of System Integrity	Civil or Criminal Penalties?	Private Right of Action Included in Breach Law?	Criminal Investigation or Publicly Available Information Exception?	Other Parties to be Notified? (Excludes State Agency Obligations)
Nebraska Neb. Rev Stat 87-801, 87-802, 87-803, 87-804, 87-805, 87-806 and 87-807 7/14/06	Unauthorized acquisition of computerized data that compromises security, confidentiality or integrity of PI unless reasonable & prompt investigation finds *no use or likely use* of PI for unauthorized purpose	Electronic	CA plus redacted or other method that makes data unreadable, unique electronic ID # or routing code with code and biometric data	Encryption, redaction or other method that makes data unreadable	Yes, applies to government, governmental subdivision, agency and instrumentalities.	No	As soon as possible and without unreasonable delay unless reasonable & prompt investigation finds no use or likely use of PI for unauthorized purpose	Yes	No	Yes, both	No
Nevada Nev. Rev. Stat. 603A.010 et seq. 10/1/05, 1/1/06 or 10/1/08 (depending on provision) Nev. Rev. Stat. 603A.215 1/1/10	Unauthorized acquisition of computerized data that ***materially*** compromises security, confidentiality or integrity of PI	Electronic	CA, but excludes last 4 numbers of SSN	Encrypted (eff. 10/1/08, must encrypt all external electronic trans-missions containing PI other than faxes; eff. 1/1/10, such encryption must be a standard adopted by an established standards setting body; this revised definition of encryption does ***not*** apply to breach determinations.)	Yes, applies to any gov't agency and institution of higher education.	Yes, shred, erase or otherwise modify PI to make unreadable or undecipherable if no longer needed. Use reasonable security measures and include security terms in contracts where PI disclosed unless subject to fed. or state law with greater protections. Effective 1/1/10, all data collectors that accept payment cards must comply with PCI Data Security Standard; also, all external electronic transmissions containing PI other than faxes must be secured using encryption and using an encryption standard adopted by an established standards setting body (e.g., NIST); also, must not transfer a data storage device containing PI beyond logical or physical controls unless using such level of encryption. Safe harbor from liability for damages if comply with revised provision, barring gross negligence or int. misconduct.	Most expedient time possible and without unreasonable delay	Yes	Yes, data collector can sue breacher	Yes, both	Consumer Reporting Agencies if notifying 1,000+ persons

*"CA" = California's initial definition of "Personal Information," which was "an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (1) Social security number, (2) Driver's license number or California Identification Card number (3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account." Ca. Civ. Code § 1798.82(e).

State, Law & Effective Date	Triggering Event (Risk / Harm or Access)	Electronic Only or Paper Included?	"Personal Information" Definition As Compared To CA Definition*	Exception for Encryption or Redaction?	Applicable to State or Government Agencies?[1]	Pre-Breach Measures Included in Breach Law?	Timing of Notification Following Determination of Scope Of Breach & Restoration Of System Integrity	Civil or Criminal Penalties?	Private Right of Action Included in Breach Law?	Criminal Investigation or Publicly Available Information Exception?	Other Parties to be Notified? (Excludes State Agency Obligations)
New Hampshire N.H. RS 359-C:19 et seq. 1/1/07, N.H.-RS 358-A:3 1/1/07 & HB 619 (amending ch. 213) 1/1/10 (PHI-related only)	Unauthorized acquisition of computerized data that compromises security or confidentiality of PI unless promptly determine that no ***misuse*** or likely misuse of PI	Electronic	CA	Encryption (unless key is also disclosed)	Yes, applies to any agency, authority, board, court, department, division, commission, institution, bureau, or other state governmental entity, or any political subdivision of the state.	As of 1/1/10, health care providers and their business associates ("BAs") will be obligated to notify affected individuals of disclosures of PHI that are allowed under federal law, but are prohibited under NH law. Under NH law, health care providers and their BAs must (i) obtain authorization for the use or disclosure of PHI for "marketing" and (ii) offer individuals an opt-out opportunity for the use or disclosure of PHI for fundraising purposes. In addition, PHI cannot be disclosed for marketing (even with an authorization) or fundraising by voice mail, unattended facsimile, or through other methods of communication that are not secure.	As soon as possible unless promptly determine that no misuse or likely misuse of PI	Yes	Yes	Yes, both	Primary regulator if subject to 358-A:3; others notify attorney general. Consumer Reporting Agencies if notifying 1,000+ consumers unless subject to GLBA
New Jersey N.J. Stat. 56:8-161-163 1/1/06	Unauthorized access to electronic files, media or data with PI that compromises security, confidentiality or integrity of PI unless investigation finds misuse of PI is not reasonably possible (must retain documentation in writing for 5 years)	Electronic	CA plus dissociated data that, if linked, would constitute PI if link accessed.	Encrypted or other method unless that renders PI unreadable or unusable	Yes, applies to "public entities", which includes the State, any county, municipality, district, public authority, public agency, and any other political subdivision or public body in the State.	Yes, destroy by shredding, erasing or otherwise modifying PI to make unreadable, undecipherable or nonreconstructable. Additional guidelines on SSN in N.J. Stat. 56:8-164.	Most expedient time possible and without unreasonable delay unless investigation finds misuse of PI is not reasonably possible (must retain documentation in writing for 5 years)	No	No	Yes, both	Div. of State Police in Dept. of Law & Public Safety ***prior*** to notification. Consumer Reporting Agencies if notifying 1,000+ persons
New Mexico											

*"CA" = California's initial definition of "Personal Information," which was "an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (1) Social security number, (2) Driver's license number or California Identification Card number (3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account." Ca. Civ. Code § 1798.82(e).

State, Law & Effective Date	Triggering Event (Risk / Harm or Access)	Electronic Only or Paper Included?	"Personal Information" Definition As Compared To CA Definition*	Exception for Encryption or Redaction?	Applicable to State or Government Agencies?[1]	Pre-Breach Measures Included in Breach Law?	Timing of Notification Following Determination of Scope Of Breach & Restoration Of System Integrity	Civil or Criminal Penalties?	Private Right of Action Included in Breach Law?	Criminal Investigation or Publicly Available Information Exception?	Other Parties to be Notified? (Excludes State Agency Obligations)
New York N.Y. Bus. Law § 899-aa 12/8/05	Unauthorized acquisition of computerized data with private information that compromises security, confidentiality or integrity of private information (e.g., stolen laptop, signs of downloading / copying or fraudulent accounts or identity theft reports)	Electronic	"Personal Information" includes name, number, personal mark or other identifier that can identify a natural person. "Private Information" = CA with PI instead of first name or first initial & last name	Encryption (unless key is also disclosed)	No	Not in breach law, but in N.Y. Gen. Bus. Law § 399-h, which prohibits a person from destroying a record with personal identifying information ("PII") unless (1) record is shredded before disposal; (2) PII contained in the record is destroyed; (3) record modified to make PII unreadable; or (4) actions consistent with commonly accepted industry practices that it reasonably believes will ensure that no unauthorized person will have access to PII in record are taken.	Most expedient time possible and without unreasonable delay	Yes	No	Yes, both	Attorney General, Consumer Protection Bd. and State Office of Cyber Security if any NY residents notified. Consumer Reporting Agencies if notifying 5,000+ persons
North Carolina N.C. Gen. Stat § 75-60 et seq 12/1/05; N.C. Gen. Stat § 132 1.10 8/1/06 NC SB 1017 (eff. 10/1/09)	Unauthorized access to and acquisition of records or data containing PI where illegal use of the PI has occurred or is reasonably likely to occur or that creates a *material* risk of harm to a consumer.	Electronic, paper or otherwise – "Records" = any material upon which written, drawn, spoken, visual or electromagnetic information or images are recorded or preserved regardless of physical form or characte-	Person's first name or first initial and last name combined with one or more of: SSN, driver's license # checking or savings account # or credit card or debit card #, PIN, digital signature, biometric data, fingerprint or passwords. Also electronic ID #, email names or addresses, parent's maiden name or any other #s if permit access to financial	Encryption (unless confidential process or key is accessed) and redaction	Yes	Yes, extensive measures required in §75-64, but excludes entities subject to GLBA, HIPAA or FCRA	Without unreasonable delay	Yes	Yes, if injured as a result of a violation	Yes, both	Consumer Protection Division of AG's Office and Consumer Reporting Agencies if notifying 1,000+ persons; *eff. 10/1/09*: Must notify the Consumer Protection Division of the AG's Office of the nature of the breach, # of consumers affected by breach, steps taken to investigate the breach, steps taken to prevent a similar

*"CA" = California's initial definition of "Personal Information," which was "an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (1) Social security number, (2) Driver's license number or California Identification Card number (3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account." Ca. Civ. Code § 1798.82(e).

State, Law & Effective Date	Triggering Event (Risk / Harm or Access)	Electronic Only or Paper Included?	"Personal Information" Definition As Compared To CA Definition*	Exception for Encryption or Redaction?	Applicable to State or Government Agencies?[1]	Pre-Breach Measures Included in Breach Law?	Timing of Notification Following Determination of Scope Of Breach & Restoration Of System Integrity	Civil or Criminal Penalties?	Private Right of Action Included in Breach Law?	Criminal Investigation or Publicly Available Information Exception?	Other Parties to be Notified? (Excludes State Agency Obligations)
		ristics	resources								breach in the future, and information regarding the timing, distribution, and content of the notice.
North Dakota N.D. Cent. Code § 51-30-01 et seq. 6/1/05	Unauthorized acquisition of computerized data giving access to PI	Electronic	CA plus DOB, mother's maiden name, employee ID# & digitized or electronic signature	Encryption or other method that renders PI unreadable or unusable	No	No	Most expedient time possible and without unreasonable delay	Yes	No	Yes, both	No
Ohio Ohio Rev. Code § 1349.19 et seq., 1349.191, 1349.192 & 1347.12 (gov't agencies) 3/30/07	Unauthorized access to and acquisition of computerized data containing PI that causes, reasonably is believed to have caused or reasonably is believed will cause ***material*** risk of ID theft or other fraud	Electronic	CA plus redacted or other method that renders data elements unreadable	Encryption, redaction or other method that renders data elements unreadable	Yes	No	Without unreasonable delay, but ***no later than 45 days*** (subject to legitimate needs of law enforcement)	Yes	No	Yes, both	Consumer Reporting Agencies if notifying 1,000+ OH residents
Oklahoma Okla. Stat. § 74-3113.1, as amended by §24-161 et seq. 11/1/08	Unauthorized access and acquisition of computerized data that compromises security or confidentiality of PI maintained as part of a database regarding multiple individuals that causes or is reasonably believed to cause *identity theft or fraud*	Electronic	CA plus redacted	Encryption (unless key is disclosed) and redaction	Yes, applies to governments, governmental subdivisions, agencies, and instrumentalities.	No	Without unreasonable delay	Yes	No	Yes, both	No

*"CA" = California's initial definition of "Personal Information," which was "an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (1) Social security number, (2) Driver's license number or California Identification Card number (3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account." Ca. Civ. Code § 1798.82(e).

State, Law & Effective Date	Triggering Event (Risk / Harm or Access)	Electronic Only or Paper Included?	"Personal Information" Definition As Compared To CA Definition*	Exception for Encryption or Redaction?	Applicable to State or Government Agencies?[1]	Pre-Breach Measures Included in Breach Law?	Timing of Notification Following Determination of Scope Of Breach & Restoration Of System Integrity	Civil or Criminal Penalties?	Private Right of Action Included in Breach Law?	Criminal Investigation or Publicly Available Information Exception?	Other Parties to be Notified? (Excludes State Agency Obligations)
Oregon Or. Rev. Stat. 646A.600 et seq. 10/1/07 (Section 12 (Security Program) 10/1/07)	Unauthorized acquisition of computerized data that compromises security, confidentiality or integrity of PI unless investigation finds no reasonable likelihood of ***harm*** to OR residents (must retain documentation in writing for 5 years)	Electronic	CA plus financial account number, passport number or other US-issued ID No., or such information sufficient to permit a person to commit identity theft	Encryption (unless key is disclosed), redaction or other methods	Yes, applies to public bodies, which include state government bodies, local government bodies and special government bodies.	Provisions relating to display and use of Social Security numbers; must develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of PI, including disposal of PI no longer needed by burning, pulverizing, shredding or modifying a physical record or destroying or erasing electronic media	Most expeditious time possible and without unreasonable delay unless investigation finds no reasonable likelihood of harm to OR residents (must retain documentation in writing for 5 years)	Yes	No, but if the director of Dept. of Consumer & Business Services may require a violator to pay compensation to consumers injured by the violation upon a finding that enforcement of consumers' rights by private civil action would be so burdensome or expensive as to be impractical	Yes, both	Consumer Reporting Agencies if notifying 1,000+ OR residents
Pennsylvania 73 Pa. Cons. Stat. § 2303 6/22/06	Unauthorized access & acquisition of computerized data that ***materially*** compromises security or confidentiality of PI in database and causes or could be reasonably believed to cause loss or injury	Electronic	CA plus redacted and financial account number, etc. instead of account number, etc.	Encryption (unless key is disclosed) or redaction	Yes, applies to state agencies and political subdivisions.	No	Without unreasonable delay	Yes	No	Yes, both	Consumer Reporting Agencies if notifying 1,000+ persons

*"CA" = California's initial definition of "Personal Information," which was "an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (1) Social security number, (2) Driver's license number or California Identification Card number (3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account." Ca. Civ. Code § 1798.82(e).

State, Law & Effective Date	Triggering Event (Risk / Harm or Access)	Electronic Only or Paper Included?	"Personal Information" Definition As Compared To CA Definition*	Exception for Encryption or Redaction?	Applicable to State or Government Agencies?[1]	Pre-Breach Measures Included in Breach Law?	Timing of Notification Following Determination of Scope Of Breach & Restoration Of System Integrity	Civil or Criminal Penalties?	Private Right of Action Included in Breach Law?	Criminal Investigation or Publicly Available Information Exception?	Other Parties to be Notified? (Excludes State Agency Obligations)
Rhode Island R.I. Gen. Laws § 11-49.2-1 et seq. and 6-52-2 3/1/06	Unauthorized acquisition of computerized data that compromises security, confidentiality or integrity of PI; notification required if breach poses ***significant risk*** of identity theft	Electronic	CA	Encryption	Yes, applies to state agencies.	Yes, reasonable security procedures by owners and licensees as well as recipient if disclose unencrypted PI. Also, a business shall take reasonable steps to destroy or arrange for the destruction of a customer's PI within its custody and control that is no longer to be retained by the business by shredding, erasing, or otherwise destroying and/or modifying the PI in those records to make it unreadable or indecipherable through any means[,].	If breach poses ***significant risk*** of identity theft, most expedient time possible and without unreasonable delay	Yes	No	Criminal investigation only	No
South Carolina S.C. Code § 39-1-90 7/1/09 S.C. Code § 16-13-510	Unauthorized access to and acquisition of computerized data containing personal identifying information ("PII") that compromises the security, confidentiality, or integrity of PII when ***illegal use*** has occurred or is reasonably likely to occur or use of the information creates a ***material*** risk of harm to a resident	Electronic	CA + other numbers or information which may be used to access a person's financial accounts or numbers or information issued by a governmental or regulatory entity that will uniquely identify an individual (personal identifying information ("PII"))	Encryption, redaction, or other methods	Yes, applies to any agency, department, board, commission, committee, or institution of higher learning of the State or a political subdivision of it.	Yes, rules on disclosure of SSNs and when disposing of PII, must modify, by shredding, erasing or other means, to make it unreadable or undecipherable	Following discovery or notification of breach and most expedient time and manner possible and without unreasonable delay	Yes	Yes	Yes, both	Consumer Protection Division of Dept. of Consumer Affairs & all national Consumer Reporting Agencies if notifying 1,000+ persons
South Dakota											

*"CA" = California's initial definition of "Personal Information," which was "an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (1) Social security number, (2) Driver's license number or California Identification Card number (3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account." Ca. Civ. Code § 1798.82(e).

State, Law & Effective Date	Triggering Event (Risk / Harm or Access)	Electronic Only or Paper Included?	"Personal Information" Definition As Compared To CA Definition*	Exception for Encryption or Redaction?	Applicable to State or Government Agencies?[1]	Pre-Breach Measures Included in Breach Law?	Timing of Notification Following Determination of Scope Of Breach & Restoration Of System Integrity	Civil or Criminal Penalties?	Private Right of Action Included in Breach Law?	Criminal Investigation or Publicly Available Information Exception?	Other Parties to be Notified? (Excludes State Agency Obligations)
Tennessee Tenn. Code § 47-18-2107 7/1/05 S.B. 2793 3/22/10	Unauthorized acquisition of computerized data that *materially* compromises security, confidentiality or integrity of PI	Electronic	CA. *Eff. 3/22/10, not* notice-triggering when TN Independent Colleges & Universities Ass'n or its members are req'd by law to disclose to TN Higher Ed. Comm'n *confidential student data or records*.	Encryption	Yes, applies to any agency of the state or any of its political subdivisions.	No	Most expedient time possible and without unreasonable delay	Yes	Yes (but state agencies can't sue)	Yes, both	Consumer Reporting Agencies & credit bureaus if notifying 1,000+ persons
Texas Tex. Bus. & Com. Code §§ 521.001 et seq., eff. 4/1/09, as amended by HB No. 2004 (eff. 9/1/09) (applies to sensitive info.) (amended to apply to state agencies along with other amend-ments); Tex. Bus. & Com. Code § 72.001 et seq. (4/1/09) (applies to personal identifying info.[6])	Unauthorized acquisition of computerized data that compromises security, confidentiality or integrity of sensitive PI; *Eff. 9/1/09*, "breach of system security" will also include "data that is encrypted if the person accessing the data has the key required to decrypt the data."	Electronic	"Sensitive Personal Information" = CA (also has "Personal Identifying Information" definition). *Eff. 9/1/09*, includes information that identifies an individual and relates to (i) the physical or mental health condition; (ii) the provision of health care; or (iii) payment for the provision of health care.	Encryption (for "Sensitive PI"); *Eff. 9/1/09*, "breach of system security" will also include "data that is encrypted if the person accessing the data has the key required to decrypt the data."	Yes	Yes, a business (including non-profit athletic or sports associations) must maintain reasonable procedures & destroy by shredding, erasing or otherwise modifying PI to make unreadable, or undecipherable (exempts "financial institution" as defined by 15 USC § 6809)	As quickly as possible	Yes	Yes	Yes, both	Consumer Reporting Agencies if notifying 10,000+ persons

[6] "Personal identifying information" means an individual's first name or initial and last name in combination with one or more of the following: (A) date of birth; (B) social security number or other government-issued identification number; (C) mother's maiden name; (D) unique biometric data, including the individual's fingerprint, voice data, or retina or iris image; (E) unique electronic identification number, address, or routing code; (F) telecommunication access device as defined by Section 32.51, Penal Code, including debit or credit card information; or (G) financial institution account number or any other financial information.

*"CA" = California's initial definition of "Personal Information," which was "an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (1) Social security number, (2) Driver's license number or California Identification Card number (3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account." Ca. Civ. Code § 1798.82(e).

State, Law & Effective Date	Triggering Event (Risk / Harm or Access)	Electronic Only or Paper Included?	"Personal Information" Definition As Compared To CA Definition*	Exception for Encryption or Redaction?	Applicable to State or Government Agencies?[1]	Pre-Breach Measures Included in Breach Law?	Timing of Notification Following Determination of Scope Of Breach & Restoration Of System Integrity	Civil or Criminal Penalties?	Private Right of Action Included in Breach Law?	Criminal Investigation or Publicly Available Information Exception?	Other Parties to be Notified? (Excludes State Agency Obligations)
Utah Utah Code § 13-44-101 et seq. 1/1/07	Unauthorized acquisition of computerized data that compromises security, confidentiality or integrity of PI unless reasonable & prompt investigation finds no ***misuse*** or reasonable likelihood of misuse of PI for ***ID theft or fraud*** purpose	Electronic	CA plus other method that renders PI unreadable or unusable and financial account number, or credit or debit card number plus any required security code, access code, or password that would permit access to the person's account	Encryption or other method that renders PI unreadable or unusable	Yes, applies to a person who owns or licenses computerized data that includes personal information concerning a Utah resident.	Yes, maintain reasonable procedures & destroy by shredding, erasing or otherwise modifying PI to make indecipherable (exempts "financial institution" as defined by 15 USC § 6809)	Most expedient time possible & without unreasonable delay unless reasonable & prompt investigation finds no misuse or reasonable likelihood of misuse of PI for ID theft or fraud purposes	Yes	No	Yes, both	No
Vermont VT. Stat. Ann. Tit. 9 §§ 2430-2445 1/1/07	Unauthorized acquisition or access of computerized data that compromises security, confidentiality or integrity of PI unless misuse of PI not reasonably possible and detailed explanation provided to AG or dept. of banking, insurance, securities or health care admin. if licensed by those depts. (If later discover misuse, must notify consumers.)	Electronic	CA plus account or card #s if can be used alone, passwords, PINs or access codes alone and excludes PI that is made unreadable by being redacted or by other method; also, financial account number, etc. instead of account #, etc.	Encryption, redaction, or other method that renders PI unreadable	Yes, applies to the state, state agencies, political subdivisions of the state, public and private universities.	Yes, destroy by shredding, erasing or otherwise modifying PI to make unreadable or indecipherable when no longer needed, but excludes entities subject to GLBA, HIPAA or FCRA. PI = following information that identifies, relates to, describes, or is capable of being associated with a particular individual: his or her signature, SSN, physical characteristics or description, passport #, driver's license or state identification card #, insurance policy #, bank account #, credit card or debit card #, or any other financial information	Most expedient time possible & without unreasonable delay unless misuse of PI not reasonably possible and detailed explanation provided to Attorney General or dept. of banking, insurance, securities or health care admin. if licensed by those depts. (If later discover misuse, must notify consumers.)	Yes	No	Yes, both	Consumer Reporting Agencies if notifying 1,000+ persons (unless licensed by Title 8 by dept. of banking, insurance, securities or health care)

*"CA" = California's initial definition of "Personal Information," which was "an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (1) Social security number, (2) Driver's license number or California Identification Card number (3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account." Ca. Civ. Code § 1798.82(e).

State, Law & Effective Date	Triggering Event (Risk / Harm or Access)	Electronic Only or Paper Included?	"Personal Information" Definition As Compared To CA Definition*	Exception for Encryption or Redaction?	Applicable to State or Government Agencies?[1]	Pre-Breach Measures Included in Breach Law?	Timing of Notification Following Determination of Scope Of Breach & Restoration Of System Integrity	Civil or Criminal Penalties?	Private Right of Action Included in Breach Law?	Criminal Investigation or Publicly Available Information Exception?	Other Parties to be Notified? (Excludes State Agency Obligations)
Virginia Va. Code §18.2-186.6 7/1/08 Va. Code § 32.1-127.1:05 (added by HB 1039) (applies to govern-mental entities only) 1/1/11	Unauthorized access and acquisition of computerized data that compromises security or confidentiality of PI maintained as part of a database regarding multiple individuals that causes or is reasonably believed to cause *identity theft or other fraud.*	Electronic	CA plus financial account number, etc. instead of account number, etc. "*Medical information*" (eff. 1/1/11) means first name or first initial and last name in combination with and linked to any one or more of the following data elements: (1) Any information regarding an individual's medical or mental health history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or (2) An individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.	Encryption (unless key acquired) or redaction. For medical information (eff. 1/1/11), "Encrypted" means the transformation of data through the use of an algorithmic process into a form in which there is a low probability of assigning meaning without the use of a confidential process or key, or securing of information by another method that renders the data elements unreadable or unusable.	Yes, applies to governments, governmental subdivisions, agencies and instrumentalities.	No	Without unreasonable delay if breach believed to have caused or will cause identity theft or fraud to any VA resident. For medical info and subject to law enforcement exception, without unreasonable delay unless delayed to determine scope of breach and restore reasonable integrity of system.	Yes. For medical info, AG can bring action and impose civil penalties up to $150,000 per breach (or a series of similar breaches of a similar nature that are discovered in a single investigation).	Yes (except for state-chartered or licensed financial institutions or an entity regulated by the State Corporation Commission's Bureau of Insurance)	Yes, both	Office of the Attorney General for PI and medical information; Consumer Reporting Agencies if notifying 1,000+ persons

*"CA" = California's initial definition of "Personal Information," which was "an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (1) Social security number, (2) Driver's license number or California Identification Card number (3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account." Ca. Civ. Code § 1798.82(e).

State, Law & Effective Date	Triggering Event (Risk / Harm or Access)	Electronic Only or Paper Included?	"Personal Information" Definition As Compared To CA Definition*	Exception for Encryption or Redaction?	Applicable to State or Government Agencies?[1]	Pre-Breach Measures Included in Breach Law?	Timing of Notification Following Determination of Scope Of Breach & Restoration Of System Integrity	Civil or Criminal Penalties?	Private Right of Action Included in Breach Law?	Criminal Investigation or Publicly Available Information Exception?	Other Parties to be Notified? (Excludes State Agency Obligations)
Washington Wash. Rev. Code § 19.255.010 7/24/05 § 19.215.020, Wash. HB 1149, 7/1/10	Unauthorized acquisition of computerized data that compromises security, confidentiality or integrity of PI unless unlikely to subject customers to a risk of *criminal activity*	Electronic	CA	Encryption	No	Must take all reasonable steps to destroy[7], or arrange for the destruction of, personal financial and health information and personal identification numbers issued by government entities in an individual's records within its custody or control when the entity is disposing of records that it will no longer retain. Under *HB 1149*, if a *processor* or *business* fails to take reasonable care to guard against unauthorized access to *payment card account information* in its possession or control, and that failure is the cause of the breach, the *processor* or *business* is liable to the relevant financial institution for reasonable actual costs related to the reissuance of payment cards to WA residents. Similarly, a *vendor* will be liable to the financial institution for these costs to the extent the damages were caused by the *vendor's* negligence. A *business* is an entity that processes more than 6,000,000 credit card and debit card transactions annually, and who provides, offers, or sells	Most expedient time possible & without unreasonable delay unless unlikely to subject customers to a risk of criminal activity	No	Yes	Yes, both	No

[7] Wash. Rev. Code § 19.215.010. (2) "Destroy personal information" means shredding, erasing, or otherwise modifying personal information in records to make the personal information unreadable or undecipherable through any reasonable means. (4) "Personal financial" and "health information" mean information that is identifiable to an individual and that is commonly used for financial or health care purposes, including account numbers, access codes or passwords, information gathered for account security purposes, credit card numbers, information held for the purpose of account access or transaction initiation, or information that relates to medical history or status. (5) "Personal identification number issued by a government entity" means a tax identification number, social security number, driver's license or permit number, state identification card number issued by the department of licensing, or any other number or code issued by a government entity for the purpose of personal identification that is protected and is not available to the public under any circumstances.

*"CA" = California's initial definition of "Personal Information," which was "an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (1) Social security number, (2) Driver's license number or California Identification Card number (3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account." Ca. Civ. Code § 1798.82(e).

State, Law & Effective Date	Triggering Event (Risk / Harm or Access)	Electronic Only or Paper Included?	"Personal Information" Definition As Compared To CA Definition*	Exception for Encryption or Redaction?	Applicable to State or Government Agencies?[1]	Pre-Breach Measures Included in Breach Law?	Timing of Notification Following Determination of Scope Of Breach & Restoration Of System Integrity	Civil or Criminal Penalties?	Private Right of Action Included in Breach Law?	Criminal Investigation or Publicly Available Information Exception?	Other Parties to be Notified? (Excludes State Agency Obligations)
						goods or services to WA residents. A *processor* is any entity, other than a business, that "directly processes or transmits [payment card] account information for or on behalf of another person as part of a payment processing service." A *vendor* is any "entity that manufactures and sells software or equipment that is designed to process, transmit, or store [payment card] account information or that maintains account information that it does not own." Safe harbors granted if account info was *encrypted* at time of breach or if entity was in compliance with *PCI DSS* and validated by annual security assessment that took place no more than 1 year prior to breach.				
Washington, D.C. DC Code Ann. § 28-3851 – 3853 3/8/07	Unauthorized acquisition of computerized or other electronic data, or any equipment or device storing such data, that compromises security, confidentiality or integrity of PI	Electronic	CA plus phone number or address in combination with other elements, also credit card or debit card #s alone, account # or access codes, etc. that allow access to financial or credit account (does not use "encrypted", but rendered secure)	Rendered secure so as to be unusable	No	No	Most expedient time possible & without unreasonable delay	Yes	No	Yes, both	Consumer Reporting Agencies if notifying 1,000+ persons unless subject to GLBA's reporting requirements

*"CA" = California's initial definition of "Personal Information," which was "an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (1) Social security number, (2) Driver's license number or California Identification Card number (3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account." Ca. Civ. Code § 1798.82(e).

State, Law & Effective Date	Triggering Event (Risk / Harm or Access)	Electronic Only or Paper Included?	"Personal Information" Definition As Compared To CA Definition*	Exception for Encryption or Redaction?	Applicable to State or Government Agencies?[1]	Pre-Breach Measures Included in Breach Law?	Timing of Notification Following Determination of Scope Of Breach & Restoration Of System Integrity	Civil or Criminal Penalties?	Private Right of Action Included in Breach Law?	Criminal Investigation or Publicly Available Information Exception?	Other Parties to be Notified? (Excludes State Agency Obligations)
West Virginia W. Va. Code §§ 46A-2A-101 – 105 6/6/08	Unauthorized access and acquisition of computerized data that compromises security or confidentiality of PI maintained as part of a database regarding multiple individuals that causes or is reasonably believed to cause *identity theft or other fraud*	Electronic	CA plus financial account number (instead of account number in CA)	Encryption (unless key is acquired) or redaction	Yes, applies to governments, governmental subdivisions, agencies and instrumentalities.	No	Without unreasonable delay if breach believed to have caused or will cause identity theft or fraud to any WVa resident	Yes	No	Yes, both	Consumer Reporting Agencies if notifying 1,000+ persons
Wisconsin Wis. Stat. §134.98 3/31/06	Unauthorized acquisition of PI unless no *material* risk of identity theft or fraud	Any form	CA plus DNA profile, biometric data and excludes PI that is redacted or made unreadable by other method; also, financial account #, etc. instead of account #, etc.	Encryption , redaction or other method that renders PI unreadable	Yes, applies to the state and any office, department, independent agency, authority, institution, association, society, or other body in state government created or authorized to be created by the constitution or any law, including the legislature and the courts.	No	Within a reasonable time, not to exceed *45 days*, unless no *material* risk of identity theft or fraud	No	No	Yes, both	Consumer Reporting Agencies if notifying 1,000+ individuals
Wyoming Wyo. Stat. Ann. § 40-12-501 to 509 7/1/07	Unauthorized acquisition of computerized data that *materially* compromises security, confidentiality or integrity of PI and causes or reasonably believed to cause *loss or injury*	Electronic	"Personal Identifying Information" = CA plus Tribal ID card or Fed or state government issued ID card, but "redacted" instead of "encrypted"	Redaction such that no more than 5 digits of SSN, id card # or payment card # show	No	No	Most expedient time possible & without unreasonable delay unless reasonable & prompt investigation shows no misuse or likelihood of misuse of PI	Yes	No	Yes, both	No

*"CA" = California's initial definition of "Personal Information," which was "an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (1) Social security number, (2) Driver's license number or California Identification Card number (3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account." Ca. Civ. Code § 1798.82(e).