State	Amendment's Effective Date	General Description of Certain Key Provisions
Connecticut (S.B. No. 949)	October 1, 2015	Requires data breach notification to individuals not later than 90 days after discovery of a breach, unless less time is required under federal law. Requires the provision of appropriate identity theft prevention services and, if applicable, identity theft mitigation services, at no cost to the consumer for a period of not less than 12 months.
Illinois (S.B. No. 1833)	If signed by the Governor, it would become effective on June 1, 2016 The amendment was sent to the Governor for signature on June 29, 2015. It passed Senate on April 22, 2015, and House on May 28, 2015	Expands the definition of "personal information" to include a name in combination with health insurance information, medical information, unique biometric data, geolocation information, and consumer marketing information. Expands the definition of "personal information" to also include user name or email address, in combination with a password or a security question and answer. Requires notification to the Attorney General of data breaches involving more than 250 Illinois residents, within 30 business days from the discovery of the breach or when notice to consumers is provided, whichever comes sooner. Includes data security provisions that require data collectors to maintain reasonable security measures to protect data from unauthorized access and to maintain similar contractual provisions. Requires certain entities to post a privacy policy.
Montana (H.B. No. 74)	October 1, 2015	Expands the definition of "personal information" to include a name in combination with medical record information or a taxpayer identification number. Requires notification to the Attorney General's consumer protection office.
Nevada (A.B. No. 179)	July 1, 2015, but not applicable to data collectors or a business until July 1, 2016	Expands the definition of "personal information" to include a name in combination with medical information or a health insurance number. Expands the definition of "personal information" to include a name in combination with a user name, unique identifier, or email address, along with a password, access code, or security question and answer.
North Dakota (S.B. No. 2214)	August 1, 2015	Expands the definition of "personal information" to include a name in combination with an identification number assigned to the individual by the individual's employer in combination with any required security code, access code, or password. Requires notification to the Attorney General of data breaches involving more than 250 North Dakota residents.

State	Amendment's Effective Date	General Description of Certain Key Provisions
Oregon (S.B. No. 601)	January 1, 2016	Expands the definition of "personal information" to include a name in combination with data from automatic measurements of a consumer's physical characteristics, a consumer's health insurance policy or subscriber identification number in combination with any unique identifier that the insurance provider uses to identify the consumer, or any information about a consumer's medical history or mental or physical condition or about a health care professional's medical diagnosis or treatment of the consumer. Requires notification to the Attorney General of data breaches involving more than 250 Oregon residents.
Rhode Island (S.B. No. 134)	June 26, 2016	Expands the definition of "personal information" to include a name in combination with medical or health information, and email addresses with any required security code, access code, or password that would permit access to an individual's personal, medical, insurance, or financial account. Requires data breach notification to individuals not later than 45 days after confirmation of a breach. Requires notification to the Attorney General and major credit reporting agencies of data breaches involving more than 500 Rhode Island residents. Broadens notification obligations to include breaches involving personal information in paper as well as electronic form. Includes data security provisions that require any person who stores, collects, processes, maintains, acquires, uses, owns, or licenses personal information to implement and maintain a risk-based information security program that contains reasonable security procedures and practices appropriate in view of the size and scope of the organization, and the nature of the information and purpose for which the information is collected, and to maintain similar contractual provisions. Precludes data retention for a period longer than is reasonably required to meet the purpose for which the data was collected, or in accordance with a written retention policy. Defines "encrypted" to require the use of a 128-bit algorithmic process. Increases the penalties for knowing and willful violations to $200 per record and eliminates the $25,000 penalty limit.
Washington (H.B. No. 1078)	July 24, 2015	Broadens notification obligations to include breaches involving non-computerized personal information. Requires data breach notification to individuals not later than 45 days after the breach was discovered. Requires notification to the Attorney General and major credit reporting agencies of data breaches involving more than 500 Washington residents not later than 45 days after the breach was discovered. Provides that notification is not required if any breach is not reasonably likely to subject consumers to a risk of harm. Covered entities and financial institutions are deemed compliant provided they comply with HIPAA and GLBA, respectively.

State	Amendment's Effective Date	General Description of Certain Key Provisions
Wyoming (S.F. No. 35) (S.F. No. 36)	July 1, 2015	Requires notice be "clear and conspicuous" and include, at a minimum, the types of personal identifying information reasonably believed affected, a general description of the incident, the approximate date of the breach, the general actions taken by the company to prevent further breaches, advice directing affected persons to remain vigilant by reviewing account statements and credit monitoring reports, and whether notification was delayed as a result of law enforcement investigation. Expands the definition of "personal information" to include account number, credit card number, or debit card number in combination with any security code, access code or password, federal or state government-issued identification card, shared secrets or security tokens known for use in data-based authentication, a username, or email address in combination with a password or security question and answer, a birth or marriage certificate, medical and health insurance information, unique biometric data, and an individual taxpayer identification number.