Privacy Rights Clearinghouse

United States Data Breach Notification Laws 2023

Table of Contents

Data Breach Notification Laws 2023

Alabama

Ala. Stat. §§ 8-38-1 — 8-31-12

Effective: June 1, 2018

Definition of breach:

"Breach of security or breach is defined as the unauthorized acquisition of data in electronic form containing sensitive personally identifying information. Acquisition occurring over a period of time committed by the same entity constitutes one breach. The term does not include good faith acquisition of sensitive personally identifying information by an employee or agent of a covered entity, unless the information is used for a purpose unrelated to the business or subject to further unauthorized use; ALA. CODE § 8-38-2(1)."

Definition of personally identifiable information:

"Sensitive personally identifying information is defined as an Alabama resident's first name or first initial and last name in combination with one or more of the following with respect to the same Alabama resident: A non-truncated Social Security number or tax identification number, a non-truncated driver's license number, state-issued identification card number, passport number, military identification number, or other unique identification number issued on a government document used to verify the identity of a specific individual, a financial account number, including a bank account number, credit card number, or debit card number, in combination with any security code, access code, password, expiration date, or PIN, that is necessary to access the financial account or to conduct a transaction that will credit or debit the financial account, any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional, an individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual, a user name or email address, in combination with a password or security question and answer that would permit access to an online account affiliated with the covered entity that is reasonably likely to contain or is used to obtain sensitive personally identifying information; ALA. CODE § 8-38-2(6)."

Does the definition of “personally identifiable information” or “breach” cover:

Biometric information:	No	**Medical information:**	Yes	**Passports and/or government IDs:**	Yes	**Paper records:**	No
De-identified information:	No	**Publicly available information:**	No	**Encrypted information:**	No	**Encrypted information when the encryption key was or is likely to have been exposed:**	Yes

Does the law cover?

Individuals:	Yes	**Businesses:**	Yes	**State government agencies:**	Yes

Notice Requirements:

Is there a "risk of harm" trigger for notification? Yes

What conditions allow for notice to be delayed?

There are permitted delays for notification. If a federal or state law enforcement agency determines that notice to individuals required under this section would interfere with a criminal investigation or national security, the notice shall be delayed upon the receipt of written request of the law enforcement agency for a period that the law enforcement agency determines is necessary; ALA. CODE § 8-38-5(c)."

If there are time limits for notification, how many days are permitted?

The law provides a specific number of days permitted for notification once it is required. Except as provided in subsection (c), the covered entity shall provide notice within 45 days of the covered entity's receipt of notice from a third-party agent that a breach has occurred or upon the covered entity's determination that a breach has occurred and is reasonably likely to cause substantial harm to the individuals to whom the information relates; ALA. CODE § 8-38-5(b)."

Does the law specify how notice must be given? Yes

If yes, what must the notice include?

The law specifies what information about the breach must be included in the data breach notification. The notice shall include, at a minimum, the date, estimated date, or estimated date range of the breach, a description of the sensitive personally identifying information that was acquired by an unauthorized person as part of the breach, a general description of the actions taken by a covered entity to restore the security and confidentiality of the personal information involved in the breach, a general description of steps an affected individual can take to protect himself or herself from identity theft, and information that the individual can use to contact the covered entity to inquire about the breach; ALA. CODE § 8-38-5(d)."

Does the law permit notice by:

Mail:	Yes	**Email:**	Yes	**Website:**	Yes

Does the law require reporting to the State's Attorney General or a separate government agency under certain conditions? Yes

If a certain number of residents need to be affected for agency reporting, how many? 1000

Does agency share breach notifications? No

Does the law require reporting to consumer reporting agencies? Yes

Does the law provide exceptions for entities complying with other laws?

HIPPA	No	**GLBA**	No	**Other:**	No

Does the law provide an exception if the entity maintains its own notification procedures? No

Does the law provide a private right of action for individuals? No

Source: http://alisondb.legislature.state.al.us/alison/CodeOfAlabama/1975/174919.htm

Data Breach Notification Laws 2023

Alaska

Alaska Stat. §§ 45.48.010 — 45.48.090

Effective: July 1, 2009

Definition of breach:

"'Breach of the security' means unauthorized acquisition, or reasonable belief of unauthorized acquisition, of personal information that compromises the security, confidentiality, or integrity of the personal information maintained by the information collector; 'acquisition' includes acquisition by photocopying, facsimile, or other paper-based method; a device, including a computer, that can read, write, or store information that is represented in numerical form; or a method not identified by the previous methods; ALASKA STAT. § 45.48.090(1)."

Definition of personally identifiable information:

"'Personal information' means information in any form on an individual that is not encrypted or redacted, or is encrypted and the encryption key has been accessed or acquired, and that consists of a combination of an individual's name and one or more of the following information elements: the individual's social security number; the individual's driver's license number or state identification card number; the individual's account number, credit card number, or debit card number; if an account can only be accessed with a personal code, the number and the personal code; passwords, personal identification numbers, or other access codes for financial accounts; ALASKA STAT. § 45.48.090(7)."

Does the definition of "personally identifiable information" or "breach" cover:

Biometric information:	No	**Medical information:**	No	**Passports and/or government IDs:**	Yes	**Paper records:**	Yes
De-identified information:	No	**Publicly available information:**	No	**Encrypted information:**	No	**Encrypted information when the encryption key was or is likely to have been exposed:**	Yes

Does the law cover?

Individuals:	Yes	**Businesses:**	Yes	**State government agencies:**	Yes

Notice Requirements:

Is there a "risk of harm" trigger for notification? Yes

What conditions allow for notice to be delayed?

An information collector may delay disclosing the breach under certain conditions; ALASKA STAT. § 45.48.020."

If there are time limits for notification, how many days are permitted?

The law does not provide a specific number of days permitted for notification once it is required; ALASKA STAT. § 45.48.010(b)."

Does the law specify how notice must be given? No

If yes, what must the notice include?

The law does not specify what information about the breach must be included in the data breach notification; ALASKA STAT. § 45.48.010."

Does the law permit notice by:

Mail:	Yes	**Email:**	Yes	**Website:**	Yes

Does the law require reporting to the State's Attorney General or a separate government agency under certain conditions? No

If a certain number of residents need to be affected for agency reporting, how many? N/A

Does agency share breach notifications? No

Does the law require reporting to consumer reporting agencies? Yes

Does the law provide exceptions for entities complying with other laws?

HIPPA	No	**GLBA**	Yes	**Other:**	No

Does the law provide an exception if the entity maintains its own notification procedures? No

Does the law provide a private right of action for individuals? No

Source: https://www.akleg.gov/basis/Bill/Text/24?Hsid=HB0270A

Data Breach Notification Laws 2023

Arizona

Ariz. Rev. Stat §§ 18-551 — 18-552

Effective: December 31, 2006

Definition of breach:

The definition of 'breach', 'data breach', 'security incident' or the event that triggers notification is not explicitly defined in the provided text. However, the term "security system breach" is used to describe the event that triggers notification requirements; ARIZ. REV. STAT. § 18-552(A).

Definition of personally identifiable information:

The definition for "Personally Identifiable Information" or the information that is covered by the law is not provided in the given text.

Does the definition of "personally identifiable information" or "breach" cover:

Biometric information:	No	**Medical information:**	No	**Passports and/or government IDs:**	Yes	**Paper records:**	No
De-identified information:	No	**Publicly available information:**	No	**Encrypted information:**	No	**Encrypted information when the encryption key was or is likely to have been exposed:**	No

Does the law cover?

Individuals:	Yes	**Businesses:**	Yes	**State government agencies:**	No

Notice Requirements:

Is there a "risk of harm" trigger for notification? Yes

What conditions allow for notice to be delayed?

The law allows for delays in notification if a law enforcement agency advises that the notifications will impede a criminal investigation; ARIZ. REV. STAT. § 18-552(D).

If there are time limits for notification, how many days are permitted?

The law provides a specific number of days permitted for notification once it is required. The person that owns or licenses the computerized data must notify the individuals affected within forty-five days after the determination of a security system breach; ARIZ. REV. STAT. § 18-552(B).

Does the law specify how notice must be given? Yes

If yes, what must the notice include?

The law specifies what information about the breach must be included in the data breach notification, such as the approximate date of the breach and a brief description of the personal information included in the breach; ARIZ. REV. STAT. § 18-552(E).

Does the law permit notice by:

Mail:	Yes	**Email:**	Yes	**Website:**	Yes

Does the law require reporting to the State's Attorney General or a separate government agency under certain conditions? Yes

If a certain number of residents need to be affected for agency reporting, how many? 1000

Does agency share breach notifications? No

Does the law require reporting to consumer reporting agencies? Yes

Does the law provide exceptions for entities complying with other laws?

HIPPA	Yes	**GLBA**	Yes	**Other:**	Yes

Does the law provide an exception if the entity maintains its own notification procedures? Yes

Does the law provide a private right of action for individuals? No

Source: https://www.azleg.gov/viewdocument/?docName=https://www.azleg.gov/ars/18/00551.htm
AND https://www.azleg.gov/viewdocument/?docName=https://www.azleg.gov/ars/18/00552.htm

Arkansas

Ark. Code Ann. §§ 4-110-101 — 4-110-108

Effective: August 12, 2005

Definition of breach:

"Breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a person or business. It does not include the good faith acquisition of personal information by an employee or agent of the person or business for the legitimate purposes of the person or business if the personal information is not otherwise used or subject to further unauthorized disclosure; ARK. CODE ANN. § 4-110-103(1).

Definition of personally identifiable information:

"Personal information" means an individual's first name or first initial and his or her last name in combination with any one (1) or more of the following data elements when either the name or the data element is not encrypted or redacted: Social Security number; Driver's license number or Arkansas identification card number; Account number, credit card number, 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; Medical information; and Biometric data; ARK. CODE ANN. § 4-110-103(7).

Does the definition of "personally identifiable information" or "breach" cover:

Biometric information:	Yes	**Medical information:**	Yes	**Passports and/or government IDs:**	Yes	**Paper records:**	No
De-identified information:	No	**Publicly available information:**	No	**Encrypted information:**	No	**Encrypted information when the encryption key was or is likely to have been exposed:**	No

Does the law cover?

Individuals:	Yes	**Businesses:**	Yes	**State government agencies:**	Yes

Notice Requirements:

Is there a "risk of harm" trigger for notification? Yes

What conditions allow for notice to be delayed?

There are permitted delays for notification. The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation; ARK. CODE ANN. § 4-110-105(c)(1).

If there are time limits for notification, how many days are permitted?

The law does not provide a specific number of days permitted for notification once it is required. The disclosure shall be made in the most expedient time and manner possible and without unreasonable delay; ARK. CODE ANN. § 4-110-105(a)(2).

Does the law specify how notice must be given? No

If yes, what must the notice include?

The law does not specify what information about the breach must be included in the data breach notification; ARK. CODE ANN. § 4-110-105.

Does the law permit notice by:

Mail:	Yes	**Email:**	Yes	**Website:**	Yes

Does the law require reporting to the State's Attorney General or a separate government agency under certain conditions? Yes

If a certain number of residents need to be affected for agency reporting, how many? 1000

Does agency share breach notifications? No

Does the law require reporting to consumer reporting agencies? No

Does the law provide exceptions for entities complying with other laws?

HIPPA	Yes	**GLBA**	Yes	**Other:**	Yes

Does the law provide an exception if the entity maintains its own notification procedures? Yes

Does the law provide a private right of action for individuals? No

Source: https://www.arkleg.state.ar.us/ArkansasLaw/

California (Individual/Business)

Cal. Civ. Code §§ 1798.82

Effective: July 1, 2003

Definition of breach:

"Breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure; CAL. CIV. CODE § 1798.82(g).

Definition of personally identifiable information:

"Personal information" means 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: Social security number, Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual, Account number or 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, Medical information, Health insurance information, Unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual, Information or data collected through the use or operation of an automated license plate recognition system, as defined in Section 1798.90.5, Genetic data, A username or email address, in combination with a password or security question and answer that would permit access to an online account; CAL. CIV. CODE § 1798.82(h).

Does the definition of "personally identifiable information" or "breach" cover:

Biometric information:	Yes	**Medical information:**	Yes	**Passports and/or government IDs:**	Yes	**Paper records:**	No
De-identified information:	No	**Publicly available information:**	No	**Encrypted information:**	Yes	**Encrypted information when the encryption key was or is likely to have been exposed:**	Yes

Does the law cover?

Individuals:	Yes	**Businesses:**	Yes	**State government agencies:**	No

Notice Requirements:

Is there a "risk of harm" trigger for notification? No

What conditions allow for notice to be delayed?

The law allows for delays in notification if a law enforcement agency determines that the notification will impede a criminal investigation; CAL. CIV. CODE § 1798.82(c).

If there are time limits for notification, how many days are permitted?

The law does not provide a specific number of days for notification once it is required. It states that disclosure should be made in the most expedient time possible and without unreasonable delay; CAL. CIV. CODE § 1798.82(a).

Does the law specify how notice must be given? Yes

If yes, what must the notice include?

The law specifies what information about the breach must be included in the data breach notification; CAL. CIV. CODE § 1798.82(d)(2).

Does the law permit notice by:

Mail:	Yes	**Email:**	Yes	**Website:**	Yes

Does the law require reporting to the State's Attorney General or a separate government agency under certain conditions? Yes

If a certain number of residents need to be affected for agency reporting, how many? 500

Does agency share breach notifications? No

Does the law require reporting to consumer reporting agencies? No

Does the law provide exceptions for entities complying with other laws?

HIPPA	Yes	**GLBA**	No	**Other:**	No

Does the law provide an exception if the entity maintains its own notification procedures? Yes

Does the law provide a private right of action for individuals? No

Source: https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.82

California (Government Agency)

Cal. Civ. Code §§ 1798.29

Effective: July 1, 2003

Definition of breach:

"Breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the agency. Good faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure; CAL. CIV. CODE § 1798.29(f).

Definition of personally identifiable information:

"Personal information" means either of the following: 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, or a username or email address, in combination with a password or security question and answer that would permit access to an online account; CAL. CIV. CODE § 1798.29(g).

Does the definition of "personally identifiable information" or "breach" cover:

Biometric information:	Yes	**Medical information:**	Yes	**Passports and/or government IDs:**	Yes	**Paper records:**	No
De-identified information:	No	**Publicly available information:**	No	**Encrypted information:**	No	**Encrypted information when the encryption key was or is likely to have been exposed:**	Yes

Does the law cover?

Individuals:	No	**Businesses:**	No	**State government agencies:**	Yes

Notice Requirements:

Is there a "risk of harm" trigger for notification? No

What conditions allow for notice to be delayed?

The law permits delays for notification if a law enforcement agency determines that the notification will impede a criminal investigation; CAL. CIV. CODE § 1798.29(c).

If there are time limits for notification, how many days are permitted?

The law does not provide a specific number of days permitted for notification once it is required. It states that 'the disclosure shall be made in the most expedient time possible and without unreasonable delay'; CAL. CIV. CODE § 1798.29(a).

Does the law specify how notice must be given? Yes

If yes, what must the notice include?

The law specifies what information about the breach must be included in the data breach notification. It requires the inclusion of information such as the name and contact information of the reporting agency, a list of the types of personal information that were or are reasonably believed to have been the subject of a breach, and a general description of the breach incident, among other things; CAL. CIV. CODE § 1798.29(d)(2).

Does the law permit notice by:

Mail:	Yes	**Email:**	Yes	**Website:**	Yes

Does the law require reporting to the State's Attorney General or a separate government agency under certain conditions? Yes

If a certain number of residents need to be affected for agency reporting, how many? 5000

Does agency share breach notifications? No

Does the law require reporting to consumer reporting agencies? No

Does the law provide exceptions for entities complying with other laws?

HIPPA	No	**GLBA**	No	**Other:**	No

Does the law provide an exception if the entity maintains its own notification procedures? Yes

Does the law provide a private right of action for individuals? No

Source: https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.29

Data Breach Notification Laws 2023

Colorado

Colo. Rev. Stat. §§ 6-1-716

Effective: September 1, 2006

Definition of breach:

"'Security breach' means the unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a covered entity. Good faith acquisition of personal information by an employee or agent of a covered entity for the covered entity's business purposes is not a security breach if the personal information is not used for a purpose unrelated to the lawful operation of the business or is not subject to further unauthorized disclosure; COLO. REV. STAT. § 6-1-716(1)(h)"

Definition of personally identifiable information:

"'Personal information' means a Colorado resident's first name or first initial and last name in combination with any one or more of the following data elements that relate to the resident, when the data elements are not encrypted, redacted, or secured by any other method rendering the name or the element unreadable or unusable: Social security number; student, military, or passport identification number; driver's license number or identification card number; medical information; health insurance identification number; or biometric data; COLO. REV. STAT. § 6-1-716(1)(g)(I)"

Does the definition of "personally identifiable information" or "breach" cover:

Biometric information:	Yes	**Medical information:**	Yes	**Passports and/or government IDs:**	Yes	**Paper records:**	No
De-identified information:	No	**Publicly available information:**	No	**Encrypted information:**	No	**Encrypted information when the encryption key was or is likely to have been exposed:**	Yes

Does the law cover?

Individuals:	Yes	**Businesses:**	Yes	**State government agencies:**	No

Notice Requirements:

Is there a "risk of harm" trigger for notification? Yes

What conditions allow for notice to be delayed?

Notice required by this section may be delayed if a law enforcement agency determines that the notice will impede a criminal investigation; COLO. REV. STAT. § 6-1-716(2)(c)"

If there are time limits for notification, how many days are permitted?

Notice must be made in the most expedient time possible and without unreasonable delay, but not later than thirty days after the date of determination that a security breach occurred; COLO. REV. STAT. § 6-1-716(2)(a)"

Does the law specify how notice must be given? Yes

If yes, what must the notice include?

The law specifies that the notice to affected Colorado residents must include the date, estimated date, or estimated date range of the security breach; a description of the personal information that was acquired or reasonably believed to have been acquired as part of the security breach; information that the resident can use to contact the covered entity to inquire about the security breach; the toll-free numbers, addresses, and websites for consumer reporting agencies; the toll-free number, address, and website for the federal trade commission; and a statement that the resident can obtain information from the federal trade commission and the credit reporting agencies about fraud alerts and security freezes; COLO. REV. STAT. § 6-1-716(2)(a.2)"

Does the law permit notice by:

Mail:	Yes	**Email:**	Yes	**Website:**	Yes

Does the law require reporting to the State's Attorney General or a separate government agency under certain conditions? Yes

If a certain number of residents need to be affected for agency reporting, how many? 500

Does agency share breach notifications? No

Does the law require reporting to consumer reporting agencies? Yes

Does the law provide exceptions for entities complying with other laws?

HIPPA	No	**GLBA**	Yes	**Other:**	No

Does the law provide an exception if the entity maintains its own notification procedures? Yes

Does the law provide a private right of action for individuals? No

Source: https://leg.colorado.gov/sites/default/files/images/olls/crs2018-title-06.pdf

Connecticut

Conn. Gen. Stat §§ 36a-701b

Effective: January 1, 2006

Definition of breach:

"'Breach of security' means unauthorized access to or unauthorized acquisition of electronic files, media, databases or computerized data, containing personal information when access to the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable; Sec. 36a-701b(a)(1).

Definition of personally identifiable information:

"Personal information" means an individual's first name or first initial and last name in combination with any one, or more, of the following data: Social Security number; taxpayer identification number; identity protection personal identification number issued by the Internal Revenue Service; driver's license number, state identification card number, passport number, military identification number or other identification number issued by the government that is commonly used to verify identity; credit or debit card number; financial account number in combination with any required security code, access code or password that would permit access to such financial account; medical information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; health insurance policy number or subscriber identification number, or any unique identifier used by a health insurer to identify the individual; or biometric information consisting of data generated by electronic measurements of an individual's unique physical characteristics used to authenticate or ascertain the individual's identity, such as a fingerprint, voice print, retina or iris image; or user name or electronic mail address, in combination with a password or security question and answer that would permit access to an online account; Sec. 36a-701b(a)(2).

Does the definition of "personally identifiable information" or "breach" cover:

Biometric information:	Yes	**Medical information:**	Yes	**Passports and/or government IDs:**	Yes	**Paper records:**	No
De-identified information:	No	**Publicly available information:**	No	**Encrypted information:**	No	**Encrypted information when the encryption key was or is likely to have been exposed:**	No

Does the law cover?

Individuals:	Yes	**Businesses:**	Yes	**State government agencies:**	No

Notice Requirements:

Is there a "risk of harm" trigger for notification? Yes

What conditions allow for notice to be delayed?

The law allows for permitted delays for notification if a law enforcement agency determines that the notification will impede a criminal investigation and such law enforcement agency has made a request that the notification be delayed; Sec. 36a-701b(d).

If there are time limits for notification, how many days are permitted?

The law provides a specific number of days permitted for notification once it is required. Such notice shall be made without unreasonable delay but not later than sixty days after the discovery of such breach; Sec. 36a-701b(b)(1).

Does the law specify how notice must be given? No

If yes, what must the notice include?

The law does not specify what information about the breach must be included in the data breach notification; Sec. 36a-701b.

Does the law permit notice by:

Mail:	Yes	**Email:**	Yes	**Website:**	Yes

Does the law require reporting to the State's Attorney General or a separate government agency under certain conditions? Yes

If a certain number of residents need to be affected for agency reporting, how many? 1

Does agency share breach notifications? No

Does the law require reporting to consumer reporting agencies? No

Does the law provide exceptions for entities complying with other laws?

HIPPA	Yes	**GLBA**	No	**Other:**	No

Does the law provide an exception if the entity maintains its own notification procedures? Yes

Does the law provide a private right of action for individuals? No

Source: https://www.cga.ct.gov/current/pub/chap_669.htm#sec_36a-701b

Delaware

Del. Code Ann. tit. 6 §§ 12B-100

Effective: June 28, 2005

Definition of breach:

"Breach of security" means the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information. Good faith acquisition of personal information by an employee or agent of any person for the purposes of such person is not a breach of security, provided that the personal information is not used for an unauthorized purpose or subject to further unauthorized disclosure; § 12B-101(1).

Definition of personally identifiable information:

"Personal information" means a Delaware resident's first name or first initial and last name in combination with any 1 or more of the following data elements that relate to that individual: Social Security number, Driver's license number or state or federal identification card number, Account number, credit card number, or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial account, Passport number, A username or email address, in combination with a password or security question and answer that would permit access to an online account, Medical history, medical treatment by a health-care professional, diagnosis of mental or physical condition by a health care professional, or deoxyribonucleic acid profile, Health insurance policy number, subscriber identification number, or any other unique identifier used by a health insurer to identify the person, Unique biometric data generated from measurements or analysis of human body characteristics for authentication purposes, An individual taxpayer identification number; § 12B-101(7).

Does the definition of "personally identifiable information" or "breach" cover:

Biometric information:	Yes	**Medical information:**	Yes	**Passports and/or government IDs:**	Yes	**Paper records:**	No
De-identified information:	No	**Publicly available information:**	No	**Encrypted information:**	No	**Encrypted information when the encryption key was or is likely to have been exposed:**	Yes

Does the law cover?

Individuals:	Yes	**Businesses:**	Yes	**State government agencies:**	Yes

Notice Requirements:

Is there a "risk of harm" trigger for notification? Yes

What conditions allow for notice to be delayed?

The law allows for delays in notification under certain conditions; § 12B-102(c).

If there are time limits for notification, how many days are permitted?

Notice must be made without unreasonable delay but not later than 60 days after determination of the breach of security; § 12B-102(c).

Does the law specify how notice must be given? No

If yes, what must the notice include?

The law does not specify what information about the breach must be included in the data breach notification.

Does the law permit notice by:

Mail:	Yes	**Email:**	Yes	**Website:**	Yes

Does the law require reporting to the State's Attorney General or a separate government agency under certain conditions? Yes

If a certain number of residents need to be affected for agency reporting, how many? 500

Does agency share breach notifications? No

Does the law require reporting to consumer reporting agencies? No

Does the law provide exceptions for entities complying with other laws?

HIPPA	Yes	**GLBA**	Yes	**Other:**	Yes

Does the law provide an exception if the entity maintains its own notification procedures? Yes

Does the law provide a private right of action for individuals? No

Source: https://delcode.delaware.gov/title6/c012b/index.html

Data Breach Notification Laws 2023

Florida

Fla. Stat. § 501.171

Effective: July 1, 2014

Definition of breach:

"Breach of security" or "breach" means unauthorized access of data in electronic form containing personal information. Good faith access of personal information by an employee or agent of the covered entity does not constitute a breach of security, provided that the information is not used for a purpose unrelated to the business or subject to further unauthorized use; FLA. STAT. § 501.171(1)(a).

Definition of personally identifiable information:

"Personal information" means either of the following: An individual's first name or first initial and last name in combination with any one or more of the following data elements for that individual: A social security number; A driver license or identification card number, passport number, military identification number, or other similar number issued on a government document used to verify identity; A financial account number or credit or debit card number, in combination with any required security code, access code, or password that is necessary to permit access to an individual's financial account; Any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or An individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual. A user name or e-mail address, in combination with a password or security question and answer that would permit access to an online account; FLA. STAT. § 501.171(1)(g).

Does the definition of "personally identifiable information" or "breach" cover:

Biometric information:	No	**Medical information:**	Yes	**Passports and/or government IDs:**	Yes	**Paper records:**	Yes
De-identified information:	No	**Publicly available information:**	No	**Encrypted information:**	No	**Encrypted information when the encryption key was or is likely to have been exposed:**	No

Does the law cover?

Individuals:	No	**Businesses:**	Yes	**State government agencies:**	Yes

Notice Requirements:

Is there a "risk of harm" trigger for notification? Yes

What conditions allow for notice to be delayed?

There are permitted delays for notification. The law allows for a delay in notification if a federal, state, or local law enforcement agency determines that notice to individuals would interfere with a criminal investigation; FLA. STAT. § 501.171(4)(b).

If there are time limits for notification, how many days are permitted?

The law provides a specific number of days permitted for notification once it is required. Notice to individuals shall be made as expeditiously as practicable and without unreasonable delay, but no later than 30 days after the determination of a breach or reason to believe a breach occurred; FLA. STAT. § 501.171(4)(a).

Does the law specify how notice must be given? Yes

If yes, what must the notice include?

The law specifies what information about the breach must be included in the data breach notification. The notice to an individual with respect to a breach of security shall include, at a minimum: The date, estimated date, or estimated date range of the breach of security; A description of the personal information that was accessed or reasonably believed to have been accessed as a part of the breach of security; Information that the individual can use to contact the covered entity to inquire about the breach of security and the personal information that the covered entity maintained about the individual; FLA. STAT. § 501.171(4)(e).

Does the law permit notice by:

Mail:	Yes	**Email:**	Yes	**Website:**	Yes

Does the law require reporting to the State's Attorney General or a separate government agency under certain conditions? Yes

If a certain number of residents need to be affected for agency reporting, how many? 500

Does agency share breach notifications? No

Does the law require reporting to consumer reporting agencies? Yes

Does the law provide exceptions for entities complying with other laws?

HIPPA	No	**GLBA**	No	**Other:**	Yes

Does the law provide an exception if the entity maintains its own notification procedures? No

Does the law provide a private right of action for individuals? No

Source: http://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&Search_String=&URL=0500-0599/0501/Sections/0501.171.html

Data Breach Notification Laws 2023

Georgia

Ga. Code §§ 10-1-911 — 10-1-912

Effective: May 5, 2005

Definition of breach:

"Breach of the security of the system' means unauthorized acquisition of an individual's data that compromises the security, confidentiality, or integrity of personal information of such individual maintained by an information broker or data collector. Good faith acquisition or use of personal information by an employee or agent of an information broker or data collector for the purposes of such information broker or data collector is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure; GA. CODE ANN. § 10-1-911(1)"

Definition of personally identifiable information:

"'Personal information' means an individual's first name or first initial, and last name, address, or phone number, in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted: Social security number; Driver's license number or state identification card number; Account number, credit card number, or debit card number, if circumstances exist wherein such a number could be used without additional identifying information, access codes, or passwords; Account passwords or personal identification numbers or other access codes; or Any of the items contained in subparagraphs (A) through (D) of this paragraph when not in connection with the individual's first name or first initial and last name, if the information compromised would be sufficient to perform or attempt to perform identity theft against the person whose information was compromised; GA. CODE ANN. § 10-1-911(6)"

Does the definition of "personally identifiable information" or "breach" cover:

Biometric information:	No	**Medical information:**	No	**Passports and/or government IDs:**	Yes	**Paper records:**	No
De-identified information:	No	**Publicly available information:**	No	**Encrypted information:**	No	**Encrypted information when the encryption key was or is likely to have been exposed:**	No

Does the law cover?

Individuals:	Yes	**Businesses:**	Yes	**State government agencies:**	Yes

Notice Requirements:

Is there a "risk of harm" trigger for notification? No

What conditions allow for notice to be delayed?

The notification required by this Code section may be delayed if a law enforcement agency determines that the notification will compromise a criminal investigation; GA. CODE ANN. § 10-1-912(c)"

If there are time limits for notification, how many days are permitted?

The law does not provide a specific number of days for notification once it is required, it only mentions 'in the most expedient time possible and without unreasonable delay'; GA. CODE ANN. § 10-1-912(a)"

Does the law specify how notice must be given? No

If yes, what must the notice include?

The law does not specify what information about the breach must be included in the data breach notification; GA. CODE ANN. § 10-1-912"

Does the law permit notice by:

Mail:	Yes	**Email:**	Yes	**Website:**	Yes

Does the law require reporting to the State's Attorney General or a separate government agency under certain conditions? No

If a certain number of residents need to be affected for agency reporting, how many? N/A

Does agency share breach notifications? No

Does the law require reporting to consumer reporting agencies? Yes

Does the law provide exceptions for entities complying with other laws?

HIPPA	No	**GLBA**	No	**Other:**	No

Does the law provide an exception if the entity maintains its own notification procedures? No

Does the law provide a private right of action for individuals? No

Source: http://ga.elaws.us/law/section10-1-912

Hawaii

Haw. Rev. Stat. §§ 487N-1 — 487N-4

Effective: January 1, 2007

Definition of breach:

"Security breach" means an incident of unauthorized access to and acquisition of unencrypted or unredacted records or data containing personal information where illegal use of the personal information has occurred, or is reasonably likely to occur and that creates a risk of harm to a person. Any incident of unauthorized access to and acquisition of encrypted records or data containing personal information along with the confidential process or key constitutes a security breach; HRS § 487N-1.

Definition of personally identifiable information:

"Personal information" means 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 Hawaii identification card number; or (3) Account number, credit or debit card number, access code, or password that would permit access to an individual's financial account; HRS § 487N-1.

Does the definition of "personally identifiable information" or "breach" cover:

Biometric information:	No	**Medical information:**	No	**Passports and/or government IDs:**	Yes	**Paper records:**	Yes
De-identified information:	No	**Publicly available information:**	No	**Encrypted information:**	Yes	**Encrypted information when the encryption key was or is likely to have been exposed:**	Yes

Does the law cover?

Individuals:	No	**Businesses:**	Yes	**State government agencies:**	Yes

Notice Requirements:

Is there a "risk of harm" trigger for notification? Yes

What conditions allow for notice to be delayed?

The law allows for delays in notification if a law enforcement agency informs the business or government agency that notification may impede a criminal investigation or jeopardize national security and requests a delay; HRS § 487N-2.

If there are time limits for notification, how many days are permitted?

The law does not provide a specific number of days for notification, only that it should be made without unreasonable delay; HRS § 487N-2.

Does the law specify how notice must be given? Yes

If yes, what must the notice include?

The law specifies that the notice shall include a description of the incident, the type of personal information that was subject to the unauthorized access and acquisition, the general acts of the business or government agency to protect the personal information from further unauthorized access, a telephone number that the person may call for further information and assistance, and advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports; HRS § 487N-2.

Does the law permit notice by:

Mail:	Yes	**Email:**	Yes	**Website:**	Yes

Does the law require reporting to the State's Attorney General or a separate government agency under certain conditions? No

If a certain number of residents need to be affected for agency reporting, how many? 1000

Does agency share breach notifications? No

Does the law require reporting to consumer reporting agencies? Yes

Does the law provide exceptions for entities complying with other laws?

HIPPA	Yes	**GLBA**	Yes	**Other:**	No

Does the law provide an exception if the entity maintains its own notification procedures? No

Does the law provide a private right of action for individuals? Yes

Source: https://www.capitol.hawaii.gov/hrscurrent/Vol11_Ch0476-0490/HRS0487N/HRS_0487N-.htm

Data Breach Notification Laws 2023

Idaho

Idaho Code §§ 28-51-104 — 28-51-107

Effective: July 1, 2006

Definition of breach:

"Breach of the security of the system" means the illegal acquisition of unencrypted computerized data that materially compromises the security, confidentiality, or integrity of personal information for one (1) or more persons maintained by an agency, individual or a commercial entity. Good faith acquisition of personal information by an employee or agent of an agency, individual or a commercial entity for the purposes of the agency, individual or the commercial entity is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure; Idaho Code § 28-51-104(2).

Definition of personally identifiable information:

"Personal information" means an Idaho resident's first name or first initial and last name in combination with any one (1) or more of the following data elements that relate to the resident, when either the name or the data elements are not encrypted: (a) Social security number; (b) Driver's license number or Idaho identification card number; or (c) Account number, or credit or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial account; Idaho Code § 28-51-104(5).

Does the definition of “personally identifiable information” or “breach” cover:

Biometric information:	No	**Medical information:**	No	**Passports and/or government IDs:**	No	**Paper records:**	No
De-identified information:	No	**Publicly available information:**	No	**Encrypted information:**	No	**Encrypted information when the encryption key was or is likely to have been exposed:**	No

Does the law cover?

Individuals:	Yes	**Businesses:**	Yes	**State government agencies:**	Yes

Notice Requirements:

Is there a “risk of harm” trigger for notification? Yes

What conditions allow for notice to be delayed?

The law allows for delays in notification if a law enforcement agency advises that the notice will impede a criminal investigation; Idaho Code § 28-51-105(3).

If there are time limits for notification, how many days are permitted?

The law does not provide a specific number of days for notification, it only states that notification must be made "as soon as possible"; Idaho Code § 28-51-105(1).

Does the law specify how notice must be given? No

If yes, what must the notice include?

The law does not specify what information about the breach must be included in the data breach notification; Idaho Code § 28-51-105.

Does the law permit notice by:

Mail:	Yes	**Email:**	Yes	**Website:**	Yes

Does the law require reporting to the State's Attorney General or a separate government agency under certain conditions? Yes

If a certain number of residents need to be affected for agency reporting, how many? 1

Does agency share breach notifications? No

Does the law require reporting to consumer reporting agencies? No

Does the law provide exceptions for entities complying with other laws?

HIPPA	No	**GLBA**	No	**Other:**	No

Does the law provide an exception if the entity maintains its own notification procedures? Yes

Does the law provide a private right of action for individuals? No

Source: https://legislature.idaho.gov/statutesrules/idstat/Title28/T28CH51/

Illinois

815 Ill. Comp. Stat. 530/1 — 530/50

Effective: June 27, 2006

Definition of breach:

"Breach of the security of the system data" or "breach" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the data collector. "Breach of the security of the system data" does not include good faith acquisition of personal information by an employee or agent of the data collector for a legitimate purpose of the data collector, provided that the personal information is not used for a purpose unrelated to the data collector's business or subject to further unauthorized disclosure; 815 ILCS 530/5.

Definition of personally identifiable information:

"Personal information" means either of the following: (1) 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 or redacted or are encrypted or redacted but the keys to unencrypt or unredact or otherwise read the name or data elements have been acquired without authorization through the breach of security: (A) Social Security number. (B) Driver's license number or State identification card number. (C) Account number or credit or debit card number, or an account number or credit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account. (D) Medical information. (E) Health insurance information. (F) Unique biometric data generated from measurements or technical analysis of human body characteristics used by the owner or licensee to authenticate an individual, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data. (2) User name or email address, in combination with a password or security question and answer that would permit access to an online account, when either the user name or email address or password or security question and answer are not encrypted or redacted or are encrypted or redacted but the keys to unencrypt or unredact or otherwise read the data elements have been obtained through the breach of security; 815 ILCS 530/5.

Does the definition of “personally identifiable information” or “breach” cover:

Biometric information:	Yes	**Medical information:**	Yes	**Passports and/or government IDs:**	Yes	**Paper records:**	No
De-identified information:	No	**Publicly available information:**	No	**Encrypted information:**	Yes	**Encrypted information when the encryption key was or is likely to have been exposed:**	Yes

Does the law cover?

Individuals:	No	**Businesses:**	Yes	**State government agencies:**	Yes

Notice Requirements:

Is there a "risk of harm" trigger for notification? No

What conditions allow for notice to be delayed?

There are permitted delays for notification. The law allows for delay if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation and provides the data collector with a written request for the delay; 815 ILCS 530/10.

If there are time limits for notification, how many days are permitted?

The law does not provide a specific number of days permitted for notification once it is required. It states that notification should be made in the most expedient time possible and without unreasonable delay; 815 ILCS 530/10.

Does the law specify how notice must be given? Yes

If yes, what must the notice include?

The law specifies what information about the breach must be included in the data breach notification. The disclosure notification to an Illinois resident shall include, but need not be limited to, information as follows: (1) With respect to personal information as defined in Section 5 in paragraph (1) of the definition of "personal information": (A) the toll-free numbers and addresses for consumer reporting agencies; (B) the toll-free number, address, and website address for the Federal Trade Commission; and (C) a statement that the individual can obtain information from these sources about fraud alerts and security freezes. (2) With respect to personal information defined in Section 5 in paragraph (2) of the definition of "personal information", notice may be provided in electronic or other form directing the Illinois resident whose personal information has been breached to promptly change his or her user name or password and security question or answer, as applicable, or to take other steps appropriate to protect all online accounts for which the resident uses the same user name or email address and password or security question and answer; 815 ILCS 530/10.

Does the law permit notice by:

Mail:	Yes	**Email:**	Yes	**Website:**	Yes

Does the law require reporting to the State's Attorney General or a separate government agency under certain conditions? Yes

If a certain number of residents need to be affected for agency reporting, how many? 500

Does agency share breach notifications? Yes

Does the law require reporting to consumer reporting agencies? Yes

Does the law provide exceptions for entities complying with other laws?

HIPPA	Yes	**GLBA**	No	**Other:**	No

Does the law provide an exception if the entity maintains its own notification procedures? Yes

Does the law provide a private right of action for individuals? No

Source: http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=2702&ChapAct=815%20ILCS%20530/&ChapterID=67&ChapterName=BUSINESS+TRANSACTIONS&ActName=Personal+Information+Protection+Act.

Indiana

Ind. Code §§ 24-49-1-1 —24.4.9-5-1

Effective: July 1, 2006

Definition of breach:

"'Breach of the security of data' means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a person. The term includes the unauthorized acquisition of computerized data that have been transferred to another medium, including paper, microfilm, or a similar medium, even if the transferred data are no longer in a computerized format; IC 24-4.9-2-2"

Definition of personally identifiable information:

"'Personal information' means: (1) a Social Security number that is not encrypted or redacted; or (2) an individual's first and last names, or first initial and last name, and one (1) or more of the following data elements that are not encrypted or redacted: (A) A driver's license number. (B) A state identification card number. (C) A credit card number. (D) A financial account number or debit card number in combination with a security code, password, or access code that would permit access to the person's account; IC 24-4.9-2-10"

Does the definition of "personally identifiable information" or "breach" cover:

Biometric information:	No	**Medical information:**	No	**Passports and/or government IDs:**	Yes	**Paper records:**	Yes
De-identified information:	No	**Publicly available information:**	No	**Encrypted information:**	Yes	**Encrypted information when the encryption key was or is likely to have been exposed:**	Yes

Does the law cover?

Individuals:	Yes	**Businesses:**	Yes	**State government agencies:**	No

Notice Requirements:

Is there a "risk of harm" trigger for notification? Yes

What conditions allow for notice to be delayed?

The law allows for delay of notification if it is necessary to restore the integrity of the computer system, discover the scope of the breach, or in response to a request from the attorney general or a law enforcement agency; IC 24-4.9-3-3(a)"

If there are time limits for notification, how many days are permitted?

The law does not provide a specific number of days for notification once it is required. It states that notification should be made without unreasonable delay; IC 24-4.9-3-3(a)"

Does the law specify how notice must be given? No

If yes, what must the notice include?

The law does not specify what information about the breach must be included in the data breach notification; IC 24-4.9-3-1"

Does the law permit notice by:

Mail:	Yes	**Email:**	Yes	**Website:**	Yes

Does the law require reporting to the State's Attorney General or a separate government agency under certain conditions? Yes

If a certain number of residents need to be affected for agency reporting, how many? 1

Does agency share breach notifications? No

Does the law require reporting to consumer reporting agencies? Yes

Does the law provide exceptions for entities complying with other laws?

HIPPA	Yes	**GLBA**	Yes	**Other:**	Yes

Does the law provide an exception if the entity maintains its own notification procedures? Yes

Does the law provide a private right of action for individuals? No

Source: http://iga.in.gov/legislative/laws/2020/ic/titles/024#24-4.9

Data Breach Notification Laws 2023

Iowa

Iowa Code §§ 715C.1 — 715C.2

Effective: July 1, 2008

Definition of breach:

"Breach of security" means unauthorized acquisition of personal information maintained in computerized form by a person that compromises the security, confidentiality, or integrity of the personal information. It also includes unauthorized acquisition of personal information maintained by a person in any medium, including on paper, that was transferred by the person to that medium from computerized form and that compromises the security, confidentiality, or integrity of the personal information. Good faith acquisition of personal information by a person or that person's employee or agent for a legitimate purpose of that person is not a breach of security, provided that the personal information is not used in violation of applicable law or in a manner that harms or poses an actual threat to the security, confidentiality, or integrity of the personal information; IOWA CODE § 715C.1(1).

Definition of personally identifiable information:

"Personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements that relate to the individual if any of the data elements are not encrypted, redacted, or otherwise altered by any method or technology in such a manner that the name or data elements are unreadable or are encrypted, redacted, or otherwise altered by any method or technology but the keys to unencrypt, unredact, or otherwise read the data elements have been obtained through the breach of security: Social security number, Driver's license number or other unique identification number created or collected by a government body, Financial account number, credit card number, or debit card number in combination with any required expiration date, security code, access code, or password that would permit access to an individual's financial account, 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, Unique biometric data, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data; IOWA CODE § 715C.1(11).

Does the definition of "personally identifiable information" or "breach" cover:

Biometric information:	Yes	**Medical information:**	No	**Passports and/or government IDs:**	Yes	**Paper records:**	Yes
De-identified information:	No	**Publicly available information:**	No	**Encrypted information:**	Yes	**Encrypted information when the encryption key was or is likely to have been exposed:**	Yes

Does the law cover?

Individuals:	Yes	**Businesses:**	Yes	**State government agencies:**	Yes

Notice Requirements:

Is there a "risk of harm" trigger for notification? Yes

What conditions allow for notice to be delayed?

There are permitted delays for notification if a law enforcement agency determines that the notification will impede a criminal investigation; IOWA CODE § 715C.2(3).

If there are time limits for notification, how many days are permitted?

The law does not provide a specific number of days permitted for notification once it is required. The consumer notification shall be made in the most expeditious manner possible and without unreasonable delay; IOWA CODE § 715C.2(1).

Does the law specify how notice must be given? Yes

If yes, what must the notice include?

The law specifies what information about the breach must be included in the data breach notification; IOWA CODE § 715C.2(5).

Does the law permit notice by:

Mail:	Yes	**Email:**	Yes	**Website:**	Yes

Does the law require reporting to the State's Attorney General or a separate government agency under certain conditions? Yes

If a certain number of residents need to be affected for agency reporting, how many? 500

Does agency share breach notifications? No

Does the law require reporting to consumer reporting agencies? No

Does the law provide exceptions for entities complying with other laws?

HIPPA	Yes	**GLBA**	Yes	**Other:**	Yes

Does the law provide an exception if the entity maintains its own notification procedures? Yes

Does the law provide a private right of action for individuals? No

Source: https://www.legis.iowa.gov/docs/code/715c.pdf

Data Breach Notification Laws 2023

Kansas

Kan. Stat §§ 50-7a01 — 50-7a04

Effective: January 1, 2007

Definition of breach:

"Security breach" means the unauthorized access and acquisition of unencrypted or unredacted computerized data that compromises the security, confidentiality or integrity of personal information maintained by an individual or a commercial entity and that causes, or such individual or entity reasonably believes has caused or will cause, identity theft to any consumer; K.S.A. 2021 Supp. 50-7a01(h)

Definition of personally identifiable information:

"Personal information" means a consumer's first name or first initial and last name linked to any one or more of the following data elements that relate to the consumer, when the data elements are neither encrypted nor redacted: Social security number; driver's license number or state identification card number; or financial account number, or 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; K.S.A. 2021 Supp. 50-7a01(g)

Does the definition of "personally identifiable information" or "breach" cover:

Biometric information:	No	**Medical information:**	No	**Passports and/or government IDs:**	Yes	**Paper records:**	No
De-identified information:	No	**Publicly available information:**	No	**Encrypted information:**	No	**Encrypted information when the encryption key was or is likely to have been exposed:**	No

Does the law cover?

Individuals:	Yes	**Businesses:**	Yes	**State government agencies:**	Yes

Notice Requirements:

Is there a "risk of harm" trigger for notification? Yes

What conditions allow for notice to be delayed?

Notice required by this section may be delayed if a law enforcement agency determines that the notice will impede a criminal investigation; K.S.A. 2021 Supp. 50-7a02(c)

If there are time limits for notification, how many days are permitted?

The law does not provide a specific number of days permitted for notification once it is required; K.S.A. 2021 Supp. 50-7a02(a)

Does the law specify how notice must be given? No

If yes, what must the notice include?

The law does not specify what information about the breach must be included in the data breach notification; K.S.A. 2021 Supp. 50-7a02

Does the law permit notice by:

Mail:	Yes	**Email:**	Yes	**Website:**	Yes

Does the law require reporting to the State's Attorney General or a separate government agency under certain conditions? No

If a certain number of residents need to be affected for agency reporting, how many? N/A

Does agency share breach notifications? No

Does the law require reporting to consumer reporting agencies? Yes

Does the law provide exceptions for entities complying with other laws?

HIPPA	Yes	**GLBA**	Yes	**Other:**	Yes

Does the law provide an exception if the entity maintains its own notification procedures? Yes

Does the law provide a private right of action for individuals? No

Source: http://www.kslegislature.org/li/b2021_22/statute/050_000_0000_chapter/050_007a_0000_article/

Data Breach Notification Laws 2023

Kentucky

Ky. Rev. Stat § 365.732

Effective: January 15, 2014

Definition of breach:

"'Breach of the security of the system' means unauthorized acquisition of unencrypted and unredacted computerized data that compromises the security, confidentiality, or integrity of personally identifiable information maintained by the information holder as part of a database regarding multiple individuals that actually causes, or leads the information holder to reasonably believe has caused or will cause, identity theft or fraud against any resident of the Commonwealth of Kentucky. Good-faith acquisition of personally identifiable information by an employee or agent of the information holder for the purposes of the information holder is not a breach of the security of the system if the personally identifiable information is not used or subject to further unauthorized disclosure; 365.732 (1)(a).

Definition of personally identifiable information:

"Personally identifiable information" means an individual's first name or first initial and last name in combination with any one (1) or more of the following data elements, when the name or data element is not redacted: 1. Social Security number; 2. Driver's license number; or 3. Account number or credit or debit card number, in combination with any required security code, access code, or password to permit access to an individual's financial account; 365.732 (1)(c).

Does the definition of "personally identifiable information" or "breach" cover:

Biometric information:	No	**Medical information:**	No	**Passports and/or government IDs:**	Yes	**Paper records:**	No
De-identified information:	No	**Publicly available information:**	No	**Encrypted information:**	No	**Encrypted information when the encryption key was or is likely to have been exposed:**	No

Does the law cover?

Individuals:	Yes	**Businesses:**	Yes	**State government agencies:**	No

Notice Requirements:

Is there a "risk of harm" trigger for notification? Yes

What conditions allow for notice to be delayed?

The law allows for notification to be delayed if a law enforcement agency determines that the notification will impede a criminal investigation; 365.732 (4).

If there are time limits for notification, how many days are permitted?

The law does not provide a specific number of days for notification, instead requiring it to be made "in the most expedient time possible and without unreasonable delay"; 365.732 (2).

Does the law specify how notice must be given? No

If yes, what must the notice include?

The law does not specify what information about the breach must be included in the data breach notification; 365.732.

Does the law permit notice by:

Mail:	Yes	**Email:**	Yes	**Website:**	Yes

Does the law require reporting to the State's Attorney General or a separate government agency under certain conditions? No

If a certain number of residents need to be affected for agency reporting, how many? N/A

Does agency share breach notifications? No

Does the law require reporting to consumer reporting agencies? Yes

Does the law provide exceptions for entities complying with other laws?

HIPPA	Yes	**GLBA**	Yes	**Other:**	Yes

Does the law provide an exception if the entity maintains its own notification procedures? Yes

Does the law provide a private right of action for individuals? No

Source: https://apps.legislature.ky.gov/law/statutes/statute.aspx?id=43326

Louisiana

La. Stat. §§ 51:3071 — 51:3077

Effective: January 1, 2006

Definition of breach:

"Breach of the security of the system" means the compromise of the security, confidentiality, or integrity of computerized data that results in, or there is a reasonable likelihood to result in, the unauthorized acquisition of and access to personal information maintained by an agency or person; LA. STAT. ANN. § 51:3074(2).

Definition of personally identifiable information:

"Personal information" means the first name or first initial and last name of an individual resident of this state in combination with any one or more of the following data elements, when the name or the data element is not encrypted or redacted: Social security number, Driver's license number or state identification card number, 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, Passport number, Biometric data; LA. STAT. ANN. § 51:3074(4).

Does the definition of "personally identifiable information" or "breach" cover:

Biometric information:	Yes	**Medical information:**	No	**Passports and/or government IDs:**	Yes	**Paper records:**	No
De-identified information:	No	**Publicly available information:**	No	**Encrypted information:**	No	**Encrypted information when the encryption key was or is likely to have been exposed:**	No

Does the law cover?

Individuals:	Yes	**Businesses:**	Yes	**State government agencies:**	Yes

Notice Requirements:

Is there a "risk of harm" trigger for notification? Yes

What conditions allow for notice to be delayed?

There are permitted delays for notification as per the law; LA. STAT. ANN. § 51:3075(E), (F).

If there are time limits for notification, how many days are permitted?

The law provides a specific number of days permitted for notification once it is required, which is not later than sixty days from the discovery of the breach; LA. STAT. ANN. § 51:3075(E).

Does the law specify how notice must be given? No

If yes, what must the notice include?

The law does not specify what information about the breach must be included in the data breach notification; LA. STAT. ANN. § 51:3075.

Does the law permit notice by:

Mail:	Yes	**Email:**	Yes	**Website:**	Yes

Does the law require reporting to the State's Attorney General or a separate government agency under certain conditions? Yes

If a certain number of residents need to be affected for agency reporting, how many? N/A

Does agency share breach notifications? No

Does the law require reporting to consumer reporting agencies? No

Does the law provide exceptions for entities complying with other laws?

HIPPA	No	**GLBA**	Yes	**Other:**	No

Does the law provide an exception if the entity maintains its own notification procedures? Yes

Does the law provide a private right of action for individuals? Yes

Source: http://legis.la.gov/Legis/Law.aspx?d=322027

Data Breach Notification Laws 2023

Maine

10 Me. Stat. tit. §§ 1346 — 1350-B

Effective: January 31, 2006

Definition of breach:

"Breach of the security of the system" or "security breach" means unauthorized acquisition, release or use of an individual's computerized data that includes personal information that compromises the security, confidentiality or integrity of personal information of the individual maintained by a person; ME. REV. STAT. tit. 10, § 1347(1).

Definition of personally identifiable information:

"Personal information" means 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 or redacted: Social security number; Driver's license number or state identification card number; Account number, credit card number or debit card number, if circumstances exist wherein such a number could be used without additional identifying information, access codes or passwords; Account passwords or personal identification numbers or other access codes; ME. REV. STAT. tit. 10, § 1347(6).

Does the definition of "personally identifiable information" or "breach" cover:

Biometric information:	No	**Medical information:**	No	**Passports and/or government IDs:**	Yes	**Paper records:**	No
De-identified information:	No	**Publicly available information:**	No	**Encrypted information:**	No	**Encrypted information when the encryption key was or is likely to have been exposed:**	No

Does the law cover?

Individuals:	Yes	**Businesses:**	Yes	**State government agencies:**	Yes

Notice Requirements:

Is there a "risk of harm" trigger for notification? Yes

What conditions allow for notice to be delayed?

The law allows for delays of notification under certain circumstances; ME. REV. STAT. tit. 10, § 1348(3).

If there are time limits for notification, how many days are permitted?

If there is no delay of notification due to law enforcement investigation, the notices must be made no more than 30 days after the person becomes aware of a breach of security and identifies its scope; ME. REV. STAT. tit. 10, § 1348(1).

Does the law specify how notice must be given? No

If yes, what must the notice include?

The law does not specify what information about the breach must be included in the data breach notification; ME. REV. STAT. tit. 10, § 1348.

Does the law permit notice by:

Mail:	Yes	**Email:**	Yes	**Website:**	Yes

Does the law require reporting to the State's Attorney General or a separate government agency under certain conditions? Yes

If a certain number of residents need to be affected for agency reporting, how many? 1

Does agency share breach notifications? No

Does the law require reporting to consumer reporting agencies? Yes

Does the law provide exceptions for entities complying with other laws?

HIPPA	No	**GLBA**	No	**Other:**	No

Does the law provide an exception if the entity maintains its own notification procedures? No

Does the law provide a private right of action for individuals? No

Source: https://legislature.maine.gov/legis/statutes/10/title10ch210-Bsec0.html

Maryland

Md. Code Com. Law §§ 14-3501 — 14-3508

Effective: January 1, 2008

Definition of breach:

"Breach of the security of a system" means the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of the personal information maintained by a business; MD. CODE ANN., COM. LAW § 14–3504(a)(1).

Definition of personally identifiable information:

"Personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when the data elements are not encrypted, redacted, or otherwise protected by another method that renders the information unreadable or unusable: A Social Security number, an Individual Taxpayer Identification Number, a passport number, or other identification number issued by the federal government; A driver's license number or State identification card number; An account number, a credit card number, or a debit card number, in combination with any required security code, access code, or password, that permits access to an individual's financial account; Health information, including information about an individual's mental health; A health insurance policy or certificate number or health insurance subscriber identification number, in combination with a unique identifier used by an insurer or an employer that is self–insured, that permits access to an individual's health information; Biometric data of an individual generated by automatic measurements of an individual's biological characteristics such as a fingerprint, voice print, genetic print, retina or iris image, or other unique biological characteristic, that can be used to uniquely authenticate the individual's identity when the individual accesses a system or account; For purposes of the notifications required under § 14–3504(b)(2), (c), (d), (e), (f), and (g) of this subtitle, genetic information with respect to an individual; A user name or e–mail address in combination with a password or security question and answer that permits access to an individual's e–mail account; or For the purposes of the requirements of this title other than the notifications required under § 14–3504(b)(2), (c), (d), (e), (f), and (g) of this subtitle, genetic information with respect to an individual when the genetic information is not encrypted, redacted, or otherwise protected by another method that renders the information unreadable or unusable; MD. CODE ANN., COM. LAW § 14–3501(e)(1).

Does the definition of "personally identifiable information" or "breach" cover:

Biometric information:	Yes	**Medical information:**	Yes	**Passports and/or government IDs:**	Yes	**Paper records:**	No
De-identified information:	No	**Publicly available information:**	No	**Encrypted information:**	No	**Encrypted information when the encryption key was or is likely to have been exposed:**	No

Does the law cover?

Individuals:	No	**Businesses:**	Yes	**State government agencies:**	No

Notice Requirements:

Is there a "risk of harm" trigger for notification? Yes

What conditions allow for notice to be delayed?

The notification required under subsections (b) and (c) of this section may be delayed; MD. CODE ANN., COM. LAW § 14–3504(d)(1).

If there are time limits for notification, how many days are permitted?

The notification required under paragraph (2) of this subsection shall be given as soon as reasonably practicable, but not later than 45 days after the business discovers or is notified of the breach of the security of a system; MD. CODE ANN., COM. LAW § 14–3504(b)(3).

Does the law specify how notice must be given? Yes

If yes, what must the notice include?

The notification required under subsection (b) of this section shall include to the extent possible, a description of the categories of information that were, or are reasonably believed to have been, acquired by an unauthorized person, including which of the elements of personal information were, or are reasonably believed to have been, acquired; MD. CODE ANN., COM. LAW § 14–3504(g)(1).

Does the law permit notice by:

Mail:	Yes	**Email:**	Yes	**Website:**	Yes

Does the law require reporting to the State's Attorney General or a separate government agency under certain conditions? Yes

If a certain number of residents need to be affected for agency reporting, how many? 1

Does agency share breach notifications? No

Does the law require reporting to consumer reporting agencies? Yes

Does the law provide exceptions for entities complying with other laws?

HIPPA	Yes	**GLBA**	Yes	**Other:**	Yes

Does the law provide an exception if the entity maintains its own notification procedures? No

Does the law provide a private right of action for individuals? Not Provided

Source: https://mgaleg.maryland.gov/mgawebsite/Laws/StatuteText?article=gcl&section=14-3402&enactments=False&archived=False

Massachusetts

Mass. Gen. Laws 93H § 1 — 6

Effective: October 31, 2007

Definition of breach:

The law does not provide a specific definition for 'breach', 'data breach', 'security incident' or the event that triggers notification. However, it refers to a 'breach of security' or 'unauthorized acquisition or use' of personal information; MASS. GEN. LAWS ch. 93H § 3(a)-(b).

Definition of personally identifiable information:

The law does not provide a specific definition for "Personally Identifiable Information" or the information that is covered by the law. However, it refers to 'personal information about a resident of the commonwealth'; MASS. GEN. LAWS ch. 93H § 3(a)-(b).

Does the definition of "personally identifiable information" or "breach" cover:

Biometric information:	No	**Medical information:**	No	**Passports and/or government IDs:**	Yes	**Paper records:**	No
De-identified information:	No	**Publicly available information:**	No	**Encrypted information:**	No	**Encrypted information when the encryption key was or is likely to have been exposed:**	No

Does the law cover?

Individuals:	Yes	**Businesses:**	Yes	**State government agencies:**	Yes

Notice Requirements:

Is there a "risk of harm" trigger for notification? No

What conditions allow for notice to be delayed?

The law allows for delays in notification if a law enforcement agency determines that provision of such notice may impede a criminal investigation; MASS. GEN. LAWS ch. 93H § 4.

If there are time limits for notification, how many days are permitted?

The law does not provide a specific number of days permitted for notification once it is required. It states that notification should be provided 'as soon as practicable and without unreasonable delay'; MASS. GEN. LAWS ch. 93H § 3(a)-(b).

Does the law specify how notice must be given? Yes

If yes, what must the notice include?

The law specifies what information about the breach must be included in the data breach notification; MASS. GEN. LAWS ch. 93H § 3(b).

Does the law permit notice by:

Mail:	No	**Email:**	No	**Website:**	No

Does the law require reporting to the State's Attorney General or a separate government agency under certain conditions? Yes

If a certain number of residents need to be affected for agency reporting, how many? 1

Does agency share breach notifications? Yes

Does the law require reporting to consumer reporting agencies? Yes

Does the law provide exceptions for entities complying with other laws?

HIPPA	Yes	**GLBA**	No	**Other:**	Yes

Does the law provide an exception if the entity maintains its own notification procedures? Yes

Does the law provide a private right of action for individuals? No

Source: https://malegislature.gov/Laws/GeneralLaws/PartI/TitleXV/Chapter93H/Section3

Michigan

Mich. Comp. Laws §§ 445.61, 445.63, 445.65, 445.72

Effective: July 2, 2007

Definition of breach:

"'Breach of the security of a database' or 'security breach' means the unauthorized access and acquisition of data that compromises the security or confidentiality of personal information maintained by a person or agency as part of a database of personal information regarding multiple individuals."; MICH. COMP. LAWS § 445.63(b)

Definition of personally identifiable information:

"Personal information" means the first name or first initial and last name linked to 1 or more of the following data elements of a resident of this state: Social security number, Driver license number or state personal identification card number, Demand deposit or other financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to any of the resident's financial accounts."; MICH. COMP. LAWS § 445.63(r)

Does the definition of "personally identifiable information" or "breach" cover:

Biometric information:	Yes	**Medical information:**	No	**Passports and/or government IDs:**	Yes	**Paper records:**	No
De-identified information:	No	**Publicly available information:**	No	**Encrypted information:**	Yes	**Encrypted information when the encryption key was or is likely to have been exposed:**	Yes

Does the law cover?

Individuals:	Yes	**Businesses:**	Yes	**State government agencies:**	Yes

Notice Requirements:

Is there a "risk of harm" trigger for notification? Yes

What conditions allow for notice to be delayed?

The law allows for permitted delays for notification under certain conditions.; MICH. COMP. LAWS § 445.72(4)

If there are time limits for notification, how many days are permitted?

The law does not provide a specific number of days permitted for notification once it is required. It states that a person or agency shall provide any notice required under this section without unreasonable delay.; MICH. COMP. LAWS § 445.72(4)

Does the law specify how notice must be given? Yes

If yes, what must the notice include?

The law specifies what information about the breach must be included in the data breach notification.; MICH. COMP. LAWS § 445.72(6)

Does the law permit notice by:

Mail:	Yes	**Email:**	Yes	**Website:**	Yes

Does the law require reporting to the State's Attorney General or a separate government agency under certain conditions? No

If a certain number of residents need to be affected for agency reporting, how many? N/A

Does agency share breach notifications? No

Does the law require reporting to consumer reporting agencies? Yes

Does the law provide exceptions for entities complying with other laws?

HIPPA	Yes	**GLBA**	No	**Other:**	No

Does the law provide an exception if the entity maintains its own notification procedures? Yes

Does the law provide a private right of action for individuals? No

Source: http://www.legislature.mi.gov/(S(tinmjsu4c5cvt4ss0dwkkmwu))/mileg.aspx?page=getobject&objectname=mcl-445-72

Minnesota

Minn. Stat. §§ 325E.61, 325E.64, 8.31

Effective: July 1, 2006

Definition of breach:

"Breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security system, provided that the personal information is not used or subject to further unauthorized disclosure; 325E.61 Subd. 1(d).

Definition of personally identifiable information:

"Personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when the data element is not secured by encryption or another method of technology that makes electronic data unreadable or unusable, or was secured and the encryption key, password, or other means necessary for reading or using the data was also acquired: Social Security number; driver's license number or Minnesota identification card number; or account number or 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; 325E.61 Subd. 1(e).

Does the definition of “personally identifiable information” or “breach” cover:

Biometric information:	No	**Medical information:**	No	**Passports and/or government IDs:**	Yes	**Paper records:**	No
De-identified information:	No	**Publicly available information:**	No	**Encrypted information:**	No	**Encrypted information when the encryption key was or is likely to have been exposed:**	Yes

Does the law cover?

Individuals:	Yes	**Businesses:**	Yes	**State government agencies:**	No

Notice Requirements:

Is there a “risk of harm” trigger for notification? No

What conditions allow for notice to be delayed?

The notification may be delayed to a date certain if a law enforcement agency affirmatively determines that the notification will impede a criminal investigation; 325E.61 Subd. 1(c).

If there are time limits for notification, how many days are permitted?

The law does not provide a specific number of days permitted for notification once it is required; 325E.61 Subd. 1(a).

Does the law specify how notice must be given? No

If yes, what must the notice include?

The law does not specify what information about the breach must be included in the data breach notification; 325E.61.

Does the law permit notice by:

Mail:	Yes	**Email:**	Yes	**Website:**	Yes

Does the law require reporting to the State's Attorney General or a separate government agency under certain conditions? No

If a certain number of residents need to be affected for agency reporting, how many? N/A

Does agency share breach notifications? No

Does the law require reporting to consumer reporting agencies? Yes

Does the law provide exceptions for entities complying with other laws?

HIPPA	No	**GLBA**	No	**Other:**	No

Does the law provide an exception if the entity maintains its own notification procedures? Yes

Does the law provide a private right of action for individuals? No

Source: https://www.revisor.mn.gov/statutes/cite/325E.61

Data Breach Notification Laws 2023

Mississippi

Miss. Code § 75-24-29

Effective: July 1, 2011

Definition of breach:

"Breach of security" means unauthorized acquisition of electronic files, media, databases or computerized data containing personal information of any resident of this state when access to the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable; § 75-24-29(2)(a)

Definition of personally identifiable information:

"Personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements: (i) Social security number; (ii) Driver's license number, state identification card number or tribal identification card number; or (iii) An account number or 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; § 75-24-29(2)(b)

Does the definition of "personally identifiable information" or "breach" cover:

Biometric information:	No	**Medical information:**	No	**Passports and/or government IDs:**	Yes	**Paper records:**	No
De-identified information:	No	**Publicly available information:**	No	**Encrypted information:**	No	**Encrypted information when the encryption key was or is likely to have been exposed:**	No

Does the law cover?

Individuals:	No	**Businesses:**	Yes	**State government agencies:**	No

Notice Requirements:

Is there a "risk of harm" trigger for notification? Yes

What conditions allow for notice to be delayed?

The law allows for notification to be delayed for a reasonable period of time if a law enforcement agency determines that the notification will impede a criminal investigation or national security; § 75-24-29(5)

If there are time limits for notification, how many days are permitted?

The law does not provide a specific number of days for notification, it states that notification should be made without unreasonable delay; § 75-24-29(3)

Does the law specify how notice must be given? No

If yes, what must the notice include?

The law does not specify what information about the breach must be included in the data breach notification; § 75-24-29

Does the law permit notice by:

Mail:	Yes	**Email:**	Yes	**Website:**	Yes

Does the law require reporting to the State's Attorney General or a separate government agency under certain conditions? No

If a certain number of residents need to be affected for agency reporting, how many? N/A

Does agency share breach notifications? No

Does the law require reporting to consumer reporting agencies? No

Does the law provide exceptions for entities complying with other laws?

HIPPA	No	**GLBA**	No	**Other:**	Yes

Does the law provide an exception if the entity maintains its own notification procedures? Yes

Does the law provide a private right of action for individuals? No

Source: http://billstatus.ls.state.ms.us/documents/2020/html/HB/1300-1399/HB1314PS.htm

Missouri

Mo. Rev. Stat. § 407.1500

Effective: August 28, 2009

Definition of breach:

"Breach of security" or "breach" is defined as unauthorized access to and unauthorized acquisition of personal information maintained in computerized form by a person that compromises the security, confidentiality, or integrity of the personal information. Good faith acquisition of personal information by a person or that person's employee or agent for a legitimate purpose of that person is not a breach of security, provided that the personal information is not used in violation of applicable law or in a manner that harms or poses an actual threat to the security, confidentiality, or integrity of the personal information; MO. REV. STAT. § 407.1500(1).

Definition of personally identifiable information:

"Personal information" is defined as an individual's first name or first initial and last name in combination with any one or more of the following data elements that relate to the individual if any of the data elements are not encrypted, redacted, or otherwise altered by any method or technology in such a manner that the name or data elements are unreadable or unusable: Social Security number; Driver's license number or other unique identification number created or collected by a government body; Financial account number, credit card number, 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; 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; or Health insurance information; MO. REV. STAT. § 407.1500(9).

Does the definition of “personally identifiable information” or “breach” cover:

Biometric information:	No	**Medical information:**	Yes	**Passports and/or government IDs:**	Yes	**Paper records:**	No
De-identified information:	No	**Publicly available information:**	No	**Encrypted information:**	No	**Encrypted information when the encryption key was or is likely to have been exposed:**	No

Does the law cover?

Individuals:	Yes	**Businesses:**	Yes	**State government agencies:**	Yes

Notice Requirements:

Is there a "risk of harm" trigger for notification? Yes

What conditions allow for notice to be delayed?

The notice required by this section may be delayed if a law enforcement agency informs the person that notification may impede a criminal investigation or jeopardize national or homeland security; MO. REV. STAT. § 407.1500(2)(3).

If there are time limits for notification, how many days are permitted?

The law does not provide a specific number of days permitted for notification once it is required, it only states that the disclosure notification shall be made without unreasonable delay; MO. REV. STAT. § 407.1500(2)(1)(a).

Does the law specify how notice must be given? Yes

If yes, what must the notice include?

The notice shall at minimum include a description of the incident in general terms; the type of personal information that was obtained as a result of the breach of security; a telephone number that the affected consumer may call for further information and assistance, if one exists; contact information for consumer reporting agencies; advice that directs the affected consumer to remain vigilant by reviewing account statements and monitoring free credit reports; MO. REV. STAT. § 407.1500(2)(4).

Does the law permit notice by:

Mail:	Yes	**Email:**	Yes	**Website:**	Yes

Does the law require reporting to the State's Attorney General or a separate government agency under certain conditions? Yes

If a certain number of residents need to be affected for agency reporting, how many? 1000

Does agency share breach notifications? No

Does the law require reporting to consumer reporting agencies? Yes

Does the law provide exceptions for entities complying with other laws?

HIPPA	No	**GLBA**	Yes	**Other:**	Yes

Does the law provide an exception if the entity maintains its own notification procedures? Yes

Does the law provide a private right of action for individuals? No

Source: https://revisor.mo.gov/main/OneSection.aspx?section=407.1500&bid=23329&hl=

Data Breach Notification Laws 2023

Montana

Mont. Code §§ 30-14-1701 — 30-14-1705

Effective: March 1, 2006

Definition of breach:

"'Breach of the security of the data system' means unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of personal information maintained by the person or business and causes or is reasonably believed to cause loss or injury to a Montana resident. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the data system, provided that the personal information is not used or subject to further unauthorized disclosure; MONT. CODE ANN. § 30-14-1704(4)(a)."

Definition of personally identifiable information:

"'Personal information' means 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: social security number; driver's license number, state identification card number, or tribal identification card number; account number or 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; medical record information as defined in 33-19-104; a taxpayer identification number; or an identity protection personal identification number issued by the United States internal revenue service; MONT. CODE ANN. § 30-14-1704(4)(b)."

Does the definition of "personally identifiable information" or "breach" cover:

Biometric information:	No	**Medical information:**	Yes	**Passports and/or government IDs:**	Yes	**Paper records:**	No
De-identified information:	No	**Publicly available information:**	No	**Encrypted information:**	No	**Encrypted information when the encryption key was or is likely to have been exposed:**	No

Does the law cover?

Individuals:	Yes	**Businesses:**	Yes	**State government agencies:**	No

Notice Requirements:

Is there a "risk of harm" trigger for notification? Yes

What conditions allow for notice to be delayed?

The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation and requests a delay in notification; MONT. CODE ANN. § 30-14-1704(3)."

If there are time limits for notification, how many days are permitted?

The law does not provide a specific number of days permitted for notification once it is required; MONT. CODE ANN. § 30-14-1704."

Does the law specify how notice must be given? No

If yes, what must the notice include?

The law does not specify what information about the breach must be included in the data breach notification; MONT. CODE ANN. § 30-14-1704."

Does the law permit notice by:

Mail:	Yes	**Email:**	Yes	**Website:**	Yes

Does the law require reporting to the State's Attorney General or a separate government agency under certain conditions? Yes

If a certain number of residents need to be affected for agency reporting, how many? 1

Does agency share breach notifications? No

Does the law require reporting to consumer reporting agencies? No

Does the law provide exceptions for entities complying with other laws?

HIPPA	No	**GLBA**	No	**Other:**	No

Does the law provide an exception if the entity maintains its own notification procedures? Yes

Does the law provide a private right of action for individuals? No

Source: https://leg.mt.gov/bills/mca/title_0300/chapter_0140/part_0170/section_0040/0300-0140-0170-0040.html

Nebraska

Neb. Rev. Stat. §§ 87-801 — 807

Effective: July 14, 2006

Definition of breach:

"Breach of the security of the system means the unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by an individual or a commercial entity. Good faith acquisition of personal information by an employee or agent of an individual or a commercial entity for the purposes of the individual or the commercial entity is not a breach of the security of the system if the personal information is not used or subject to further unauthorized disclosure."; NEB. REV. STAT. § 87-802(1)

Definition of personally identifiable information:

"Personal information means either of the following: (a) A Nebraska resident's first name or first initial and last name in combination with any one or more of the following data elements that relate to the resident if either the name or the data elements are not encrypted, redacted, or otherwise altered by any method or technology in such a manner that the name or data elements are unreadable: (i) Social security number; (ii) Motor vehicle operator's license number or state identification card number; (iii) Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial account; (iv) Unique electronic identification number or routing code, in combination with any required security code, access code, or password; or (v) Unique biometric data, such as a fingerprint, voice print, or retina or iris image, or other unique physical representation; or (b) A user name or email address, in combination with a password or security question and answer, that would permit access to an online account."; NEB. REV. STAT. § 87-802(5)

Does the definition of “personally identifiable information” or “breach” cover:

Biometric information:	Yes	**Medical information:**	No	**Passports and/or government IDs:**	Yes	**Paper records:**	No
De-identified information:	No	**Publicly available information:**	No	**Encrypted information:**	No	**Encrypted information when the encryption key was or is likely to have been exposed:**	Yes

Does the law cover?

Individuals:	Yes	**Businesses:**	Yes	**State government agencies:**	Yes

Notice Requirements:

Is there a "risk of harm" trigger for notification? Yes

What conditions allow for notice to be delayed?

Notice required by this section may be delayed if a law enforcement agency determines that the notice will impede a criminal investigation; NEB. REV. STAT. § 87-803(4)

If there are time limits for notification, how many days are permitted?

The law does not provide a specific number of days permitted for notification once it is required; NEB. REV. STAT. § 87-803(1)

Does the law specify how notice must be given? No

If yes, what must the notice include?

The law does not specify what information about the breach must be included in the data breach notification; NEB. REV. STAT. § 87-803

Does the law permit notice by:

Mail:	Yes	**Email:**	Yes	**Website:**	Yes

Does the law require reporting to the State's Attorney General or a separate government agency under certain conditions? Yes

If a certain number of residents need to be affected for agency reporting, how many? 1

Does agency share breach notifications? No

Does the law require reporting to consumer reporting agencies? No

Does the law provide exceptions for entities complying with other laws?

HIPPA	No	**GLBA**	No	**Other:**	Yes

Does the law provide an exception if the entity maintains its own notification procedures? Yes

Does the law provide a private right of action for individuals? No

Source: http://nebraskalegislature.gov/laws/statutes.php?statute=87-801

Data Breach Notification Laws 2023

Nevada

Nev. Rev. Stat. §§ 603A.010—603A.040 AND Nev. Rev. Stat. §§ 603A.210—603A.220

Effective: October 1, 2005 and January 1, 2006

Definition of breach:

"Breach of the security of the system data" means unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of personal information maintained by the data collector; NRS 603A.020.

Definition of personally identifiable information:

"Personal information" means a natural person's first name or first initial and last name in combination with any one or more of the following data elements, when the name and data elements are not encrypted: Social security number, Driver's license number, driver authorization card number or identification card number, Account number, credit card number or debit card number, in combination with any required security code, access code or password that would permit access to the person's financial account, A medical identification number or a health insurance identification number, A user name, unique identifier or electronic mail address in combination with a password, access code or security question and answer that would permit access to an online account; NRS 603A.040.

Does the definition of "personally identifiable information" or "breach" cover:

Biometric information:	No	**Medical information:**	Yes	**Passports and/or government IDs:**	Yes	**Paper records:**	No
De-identified information:	No	**Publicly available information:**	No	**Encrypted information:**	No	**Encrypted information when the encryption key was or is likely to have been exposed:**	No

Does the law cover?

Individuals:	No	**Businesses:**	Yes	**State government agencies:**	Yes

Notice Requirements:

Is there a "risk of harm" trigger for notification? No

What conditions allow for notice to be delayed?

The law does not explicitly mention permitted delays for notification; NRS 603A.020.

If there are time limits for notification, how many days are permitted?

The law does not provide a specific number of days permitted for notification once it is required; NRS 603A.020.

Does the law specify how notice must be given? No

If yes, what must the notice include?

The law does not specify what information about the breach must be included in the data breach notification; NRS 603A.020.

Does the law permit notice by:

Mail:	No	**Email:**	No	**Website:**	No

Does the law require reporting to the State's Attorney General or a separate government agency under certain conditions? Yes

If a certain number of residents need to be affected for agency reporting, how many? N/A

Does agency share breach notifications? No

Does the law require reporting to consumer reporting agencies? No

Does the law provide exceptions for entities complying with other laws?

HIPPA	No	**GLBA**	Yes	**Other:**	No

Does the law provide an exception if the entity maintains its own notification procedures? No

Does the law provide a private right of action for individuals? No

Source: https://www.leg.state.nv.us/NRS/NRS-603A.html

New Hampshire

N.H. Rev. Stat. §§ 359-C:19, C:20, C:21; 358-A:4; 332-I:1—332-I:6 AND N.H. Rev. Stat. §§ 189:65, 189:66

Effective: January 1, 2007

Definition of breach:

"'Security breach' means unauthorized acquisition of computerized data that compromises the security or confidentiality of personal information maintained by a person doing business in this state. Good faith acquisition of personal information by an employee or agent of a person for the purposes of the person's business shall not be considered a security breach, provided that the personal information is not used or subject to further unauthorized disclosure; 359-C:19 V."

Definition of personally identifiable information:

"'Personal information' means an individual's first name or 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 other government identification number. (3) Account number, credit card number, 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; 359-C:19 IV."

Does the definition of "personally identifiable information" or "breach" cover:

Biometric information:	No	**Medical information:**	No	**Passports and/or government IDs:**	Yes	**Paper records:**	No
De-identified information:	No	**Publicly available information:**	No	**Encrypted information:**	No	**Encrypted information when the encryption key was or is likely to have been exposed:**	Yes

Does the law cover?

Individuals:	Yes	**Businesses:**	Yes	**State government agencies:**	Yes

Notice Requirements:

Is there a "risk of harm" trigger for notification? Yes

What conditions allow for notice to be delayed?

The law allows for notification to be delayed if a law enforcement agency, or national or homeland security agency determines that the notification will impede a criminal investigation or jeopardize national or homeland security; 359-C:20 II."

If there are time limits for notification, how many days are permitted?

The law does not provide a specific number of days for notification, it only states that notification must be made 'as soon as possible'; 359-C:20 I(a)."

Does the law specify how notice must be given? Yes

If yes, what must the notice include?

The law specifies what information about the breach must be included in the data breach notification; 359-C:20 IV."

Does the law permit notice by:

Mail:	Yes	**Email:**	Yes	**Website:**	Yes

Does the law require reporting to the State's Attorney General or a separate government agency under certain conditions? Yes

If a certain number of residents need to be affected for agency reporting, how many? 1

Does agency share breach notifications? No

Does the law require reporting to consumer reporting agencies? Yes

Does the law provide exceptions for entities complying with other laws?

HIPPA	No	**GLBA**	Yes	**Other:**	No

Does the law provide an exception if the entity maintains its own notification procedures? Yes

Does the law provide a private right of action for individuals? Yes

Source: https://www.gencourt.state.nh.us/rsa/html/xxxi/359-c/359-c-mrg.htm

New Jersey

N.J. Stat. §§ 56:8-161—56:8-166

Effective: January 1, 2006

Definition of breach:

"Breach of security" means unauthorized access to electronic files, media or data containing personal information that compromises the security, confidentiality or integrity of personal information when access to the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable; C.56:8-161.

Definition of personally identifiable information:

"Personal information" means an individual's first name or first initial and last name linked with any one or more of the following data elements: (1) Social Security number; (2) driver's license number or State identification card number; (3) account number or 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; or (4) user name, email address, or any other account holder identifying information, in combination with any password or security question and answer that would permit access to an online account; C.56:8-161.

Does the definition of "personally identifiable information" or "breach" cover:

Biometric information:	No	**Medical information:**	No	**Passports and/or government IDs:**	Yes	**Paper records:**	No
De-identified information:	No	**Publicly available information:**	No	**Encrypted information:**	No	**Encrypted information when the encryption key was or is likely to have been exposed:**	No

Does the law cover?

Individuals:	No	**Businesses:**	Yes	**State government agencies:**	Yes

Notice Requirements:

Is there a "risk of harm" trigger for notification? Yes

What conditions allow for notice to be delayed?

The notification required by this section shall be delayed if a law enforcement agency determines that the notification will impede a criminal or civil investigation; C.56:8-163.

If there are time limits for notification, how many days are permitted?

The law does not provide a specific number of days permitted for notification once it is required; C.56:8-163.

Does the law specify how notice must be given? No

If yes, what must the notice include?

The law does not specify what information about the breach must be included in the data breach notification; C.56:8-163.

Does the law permit notice by:

Mail:	Yes	**Email:**	Yes	**Website:**	Yes

Does the law require reporting to the State's Attorney General or a separate government agency under certain conditions? No

If a certain number of residents need to be affected for agency reporting, how many? 1

Does agency share breach notifications? No

Does the law require reporting to consumer reporting agencies? Yes

Does the law provide exceptions for entities complying with other laws?

HIPPA	No	**GLBA**	No	**Other:**	No

Does the law provide an exception if the entity maintains its own notification procedures? Yes

Does the law provide a private right of action for individuals? No

Source: https://lis.njleg.state.nj.us/nxt/gateway.dll?f=templates&fn=default.htm&vid=Publish:10.1048/Enu

New Mexico

N.M. Stat. §§ 57-12C-1 —57-12C-12

Effective: June 16, 2017

Definition of breach:

"'Security breach' means the unauthorized acquisition of unencrypted computerized data, or of encrypted computerized data and the confidential process or key used to decrypt the encrypted computerized data, that compromises the security, confidentiality or integrity of personal identifying information maintained by a person. 'Security breach' does not include the good-faith acquisition of personal identifying information by an employee or agent of a person for a legitimate business purpose of the person; provided that the personal identifying information is not subject to further unauthorized disclosure; 57-12C-2(D) NMSA 1978"

Definition of personally identifiable information:

"'Personal identifying information' means an individual's first name or first initial and last name in combination with one or more of the following data elements that relate to the individual, when the data elements are not protected through encryption or redaction or otherwise rendered unreadable or unusable: (a) social security number; (b) driver's license number; (c) government-issued identification number; (d) account number, credit card number or debit card number in combination with any required security code, access code or password that would permit access to a person's financial account; or (e) biometric data; 57-12C-2(C) NMSA 1978"

Does the definition of "personally identifiable information" or "breach" cover:

Biometric information:	Yes	**Medical information:**	No	**Passports and/or government IDs:**	Yes	**Paper records:**	No
De-identified information:	No	**Publicly available information:**	No	**Encrypted information:**	Yes	**Encrypted information when the encryption key was or is likely to have been exposed:**	Yes

Does the law cover?

Individuals:	Yes	**Businesses:**	Yes	**State government agencies:**	Yes

Notice Requirements:

Is there a "risk of harm" trigger for notification? Yes

What conditions allow for notice to be delayed?

There are permitted delays for notification if a law enforcement agency determines that the notification will impede a criminal investigation or if necessary to determine the scope of the security breach and restore the integrity, security and confidentiality of the data system; 57-12C-9 NMSA 1978

If there are time limits for notification, how many days are permitted?

The law provides a specific number of days permitted for notification once it is required. Notification should be made in the most expedient time possible, but not later than forty-five calendar days following discovery of the security breach; 57-12C-6(A) NMSA 1978

Does the law specify how notice must be given? Yes

If yes, what must the notice include?

The law specifies what information about the breach must be included in the data breach notification; 57-12C-7 NMSA 1978

Does the law permit notice by:

Mail:	Yes	**Email:**	Yes	**Website:**	Yes

Does the law require reporting to the State's Attorney General or a separate government agency under certain conditions? Yes

If a certain number of residents need to be affected for agency reporting, how many? 1000

Does agency share breach notifications? No

Does the law require reporting to consumer reporting agencies? Yes

Does the law provide exceptions for entities complying with other laws?

HIPPA	Yes	**GLBA**	Yes	**Other:**	No

Does the law provide an exception if the entity maintains its own notification procedures? Yes

Does the law provide a private right of action for individuals? No

Source: https://nmonesource.com/nmos/nmsa/en/item/4423/index.do#!b/57-12C-1

New York

N.Y. Gen. Bus. Laws §899-aa

Effective: December 7, 2005

Definition of breach:

"Breach of the security of the system" shall mean unauthorized access to or acquisition of, or access to or acquisition without valid authorization, of computerized data that compromises the security, confidentiality, or integrity of private information maintained by a business. Good faith access to, or acquisition of, private information by an employee or agent of the business for the purposes of the business is not a breach of the security of the system, provided that the private information is not used or subject to unauthorized disclosure; GBS § 899-aa(1)(c).

Definition of personally identifiable information:

"Personal information" shall mean any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person; GBS § 899-aa(1)(a).

Does the definition of "personally identifiable information" or "breach" cover:

Biometric information:	Yes	**Medical information:**	No	**Passports and/or government IDs:**	Yes	**Paper records:**	No
De-identified information:	No	**Publicly available information:**	No	**Encrypted information:**	Yes	**Encrypted information when the encryption key was or is likely to have been exposed:**	Yes

Does the law cover?

Individuals:	Yes	**Businesses:**	Yes	**State government agencies:**	No

Notice Requirements:

Is there a "risk of harm" trigger for notification? Yes

What conditions allow for notice to be delayed?

The notification required by this section may be delayed if a law enforcement agency determines that such notification impedes a criminal investigation; GBS § 899-aa(4).

If there are time limits for notification, how many days are permitted?

The law does not provide a specific number of days permitted for notification once it is required; GBS § 899-aa.

Does the law specify how notice must be given? Yes

If yes, what must the notice include?

The law specifies that the notice shall include contact information for the person or business making the notification, the telephone numbers and websites of the relevant state and federal agencies that provide information regarding security breach response and identity theft prevention and protection information, and a description of the categories of information that were, or are reasonably believed to have been, accessed or acquired by a person without valid authorization; GBS § 899-aa(7).

Does the law permit notice by:

Mail:	Yes	**Email:**	Yes	**Website:**	Yes

Does the law require reporting to the State's Attorney General or a separate government agency under certain conditions? Yes

If a certain number of residents need to be affected for agency reporting, how many? 1

Does agency share breach notifications? No

Does the law require reporting to consumer reporting agencies? Yes

Does the law provide exceptions for entities complying with other laws?

HIPPA	Yes	**GLBA**	Yes	**Other:**	Yes

Does the law provide an exception if the entity maintains its own notification procedures? No

Does the law provide a private right of action for individuals? No

Source: https://www.nysenate.gov/legislation/laws/GBS/899-AA

Data Breach Notification Laws 2023

North Carolina

N.C. Gen. Stat. §§ 75-61, 75-65

Effective: December 1, 2005

Definition of breach:

"Security breach" is defined as an incident of unauthorized access to and acquisition of unencrypted and unredacted records or data containing personal information where illegal use of the personal information has occurred or is reasonably likely to occur or that creates a material risk of harm to a consumer. Any incident of unauthorized access to and acquisition of encrypted records or data containing personal information along with the confidential process or key shall constitute a security breach; N.C. GEN. STAT. § 75-61(14).

Definition of personally identifiable information:

"Personal information" is defined as a person's first name or first initial and last name in combination with identifying information as defined in G.S. 14-113.20(b). Personal information does not include publicly available directories containing information an individual has voluntarily consented to have publicly disseminated or listed, including name, address, and telephone number, and does not include information made lawfully available to the general public from federal, state, or local government records; N.C. GEN. STAT. § 75-61(10).

Does the definition of "personally identifiable information" or "breach" cover:

Biometric information:	No	**Medical information:**	No	**Passports and/or government IDs:**	No	**Paper records:**	Yes
De-identified information:	No	**Publicly available information:**	No	**Encrypted information:**	No	**Encrypted information when the encryption key was or is likely to have been exposed:**	Yes

Does the law cover?

Individuals:	No	**Businesses:**	Yes	**State government agencies:**	No

Notice Requirements:

Is there a "risk of harm" trigger for notification? Yes

What conditions allow for notice to be delayed?

The law allows for delays in notification consistent with the legitimate needs of law enforcement and any measures necessary to determine sufficient contact information, determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system; N.C. GEN. STAT. § 75-65(a).

If there are time limits for notification, how many days are permitted?

The law does not provide a specific number of days for notification once it is required, it only states that notification should be made without unreasonable delay; N.C. GEN. STAT. § 75-65(a).

Does the law specify how notice must be given? Yes

If yes, what must the notice include?

The law specifies that the notice should include a description of the incident, the type of personal information that was subject to the unauthorized access and acquisition, and the general acts of the business to protect the personal information from further unauthorized access, among other things; N.C. GEN. STAT. § 75-65(d).

Does the law permit notice by:

Mail:	Yes	**Email:**	Yes	**Website:**	Yes

Does the law require reporting to the State's Attorney General or a separate government agency under certain conditions? Yes

If a certain number of residents need to be affected for agency reporting, how many? 1

Does agency share breach notifications? No

Does the law require reporting to consumer reporting agencies? Yes

Does the law provide exceptions for entities complying with other laws?

HIPPA	No	**GLBA**	No	**Other:**	Yes

Does the law provide an exception if the entity maintains its own notification procedures? No

Does the law provide a private right of action for individuals? No

Source: https://www.ncleg.net/EnactedLegislation/Statutes/HTML/BySection/Chapter_75/GS_75-65.html

North Dakota

N.D. Cent. Code §§ 51-30-01—51-20-07

Effective: June 1, 2005

Definition of breach:

"Breach of the security system" means unauthorized acquisition of computerized data when access to personal information has not been secured by encryption or by any other method or technology that renders the electronic files, media, or databases unreadable or unusable. Good-faith acquisition of personal information by an employee or agent of the person is not a breach of the security of the system, if the personal information is not used or subject to further unauthorized disclosure; N.D. CENT. CODE § 51-30-01(1).

Definition of personally identifiable information:

"Personal information" means an individual's first name or first initial and last name in combination with any of the following data elements, when the name and the data elements are not encrypted: The individual's social security number; The operator's license number assigned to an individual by the department of transportation under section 39-06-14; A nondriver color photo identification card number assigned to the individual by the department of transportation under section 39-06-03.1; The individual's financial institution account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial accounts; The individual's date of birth; The maiden name of the individual's mother; Medical information; Health insurance information; An identification number assigned to the individual by the individual's employer in combination with any required security code, access code, or password; or The individual's digitized or other electronic signature; N.D. CENT. CODE § 51-30-01(4).

Does the definition of “personally identifiable information” or “breach” cover:

Biometric information:	No	**Medical information:**	Yes	**Passports and/or government IDs:**	Yes	**Paper records:**	No
De-identified information:	No	**Publicly available information:**	No	**Encrypted information:**	No	**Encrypted information when the encryption key was or is likely to have been exposed:**	No

Does the law cover?

Individuals:	Yes	**Businesses:**	Yes	**State government agencies:**	No

Notice Requirements:

Is there a "risk of harm" trigger for notification? No

What conditions allow for notice to be delayed?

The law allows for delayed notification if a law enforcement agency determines that the notification will impede a criminal investigation; N.D. CENT. CODE § 51-30-04.

If there are time limits for notification, how many days are permitted?

The law does not provide a specific number of days for notification, only that it must be made in the most expedient time possible and without unreasonable delay; N.D. CENT. CODE § 51-30-02.

Does the law specify how notice must be given? No

If yes, what must the notice include?

The law does not specify what information about the breach must be included in the data breach notification; N.D. CENT. CODE § 51-30.

Does the law permit notice by:

Mail:	Yes	**Email:**	Yes	**Website:**	Yes

Does the law require reporting to the State's Attorney General or a separate government agency under certain conditions? Yes

If a certain number of residents need to be affected for agency reporting, how many? 250

Does agency share breach notifications? No

Does the law require reporting to consumer reporting agencies? No

Does the law provide exceptions for entities complying with other laws?

HIPPA	Yes	**GLBA**	No	**Other:**	No

Does the law provide an exception if the entity maintains its own notification procedures? Yes

Does the law provide a private right of action for individuals? No

Source: https://www.ndlegis.gov/cencode/t51c30.pdf

Ohio (Government Agencies)

Ohio Rev. Code Ann. §§ 1347.12, 1349.191—1349.192

Effective: February 17, 2006

Definition of breach:

"Breach of the security of the system" means unauthorized access to and acquisition of computerized data that compromises the security or confidentiality of personal information owned or licensed by a state agency or an agency of a political subdivision and that causes, reasonably is believed to have caused, or reasonably is believed will cause a material risk of identity theft or other fraud to the person or property of a resident of this state; R.C. §1347.12(A)(2)(a)

Definition of personally identifiable information:

"Personal information" means, notwithstanding section 1347.01 of the Revised Code, an individual's name, consisting of the individual's first name or first initial and last name, in combination with and linked to any one or more of the following data elements, when the data elements are not encrypted, redacted, or altered by any method or technology in such a manner that the data elements are unreadable: Social security number; Driver's license number or state identification card number; Account number or credit or debit card number, in combination with and linked to any required security code, access code, or password that would permit access to an individual's financial account; R.C. §1347.12(A)(6)(a)

Does the definition of "personally identifiable information" or "breach" cover:

Biometric information:	No	**Medical information:**	No	**Passports and/or government IDs:**	Yes	**Paper records:**	No
De-identified information:	No	**Publicly available information:**	No	**Encrypted information:**	No	**Encrypted information when the encryption key was or is likely to have been exposed:**	No

Does the law cover?

Individuals:	No	**Businesses:**	No	**State government agencies:**	Yes

Notice Requirements:

Is there a "risk of harm" trigger for notification? Yes

What conditions allow for notice to be delayed?

The law allows for delays in notification for law enforcement purposes or to determine the scope of the breach and restore the reasonable integrity of the data system; R.C. §1347.12(D) & R.C. §1347.12(B)(2)

If there are time limits for notification, how many days are permitted?

The law requires notification to be made in the most expedient time possible but not later than forty-five days following discovery or notification of the breach; R.C. §1347.12(B)(2)

Does the law specify how notice must be given? No

If yes, what must the notice include?

The law does not specify what information about the breach must be included in the data breach notification; R.C. §1347.12

Does the law permit notice by:

Mail:	Yes	**Email:**	Yes	**Website:**	Yes

Does the law require reporting to the State's Attorney General or a separate government agency under certain conditions? No

If a certain number of residents need to be affected for agency reporting, how many? N/A

Does agency share breach notifications? No

Does the law require reporting to consumer reporting agencies? Yes

Does the law provide exceptions for entities complying with other laws?

HIPPA	No	**GLBA**	No	**Other:**	No

Does the law provide an exception if the entity maintains its own notification procedures? No

Does the law provide a private right of action for individuals? No

Source: https://codes.ohio.gov/ohio-revised-code/section-1347.12

Ohio (Private Disclosures)

Ohio Rev. Code Ann. §§ 1349.19, 1349.191—1349.192

Effective: February 17, 2006

Definition of breach:

"Breach of the security of the system" means unauthorized access to and acquisition of computerized data that compromises the security or confidentiality of personal information owned or licensed by a person and that causes, reasonably is believed to have caused, or reasonably is believed will cause a material risk of identity theft or other fraud to the person or property of a resident of this state; R.C. §1349.19(A)(1)(a)

Definition of personally identifiable information:

"Personal information" means an individual's name, consisting of the individual's first name or first initial and last name, in combination with and linked to any one or more of the following data elements, when the data elements are not encrypted, redacted, or altered by any method or technology in such a manner that the data elements are unreadable: Social security number; Driver's license number or state identification card number; Account number or credit or debit card number, in combination with and linked to any required security code, access code, or password that would permit access to an individual's financial account; R.C. §1349.19(A)(7)(a)

Does the definition of "personally identifiable information" or "breach" cover:

Biometric information:	No	**Medical information:**	No	**Passports and/or government IDs:**	Yes	**Paper records:**	No
De-identified information:	No	**Publicly available information:**	No	**Encrypted information:**	No	**Encrypted information when the encryption key was or is likely to have been exposed:**	No

Does the law cover?

Individuals:	Yes	**Businesses:**	Yes	**State government agencies:**	No

Notice Requirements:

Is there a "risk of harm" trigger for notification? Yes

What conditions allow for notice to be delayed?

The law allows for delays in notification under certain conditions; R.C. §1349.19(D)

If there are time limits for notification, how many days are permitted?

The person shall make the disclosure in the most expedient time possible but not later than forty-five days following its discovery or notification of the breach; R.C. §1349.19(B)(2)

Does the law specify how notice must be given? No

If yes, what must the notice include?

The law does not specify what information about the breach must be included in the data breach notification; R.C. §1349.19

Does the law permit notice by:

Mail:	Yes	**Email:**	Yes	**Website:**	Yes

Does the law require reporting to the State's Attorney General or a separate government agency under certain conditions? No

If a certain number of residents need to be affected for agency reporting, how many? N/A

Does agency share breach notifications? No

Does the law require reporting to consumer reporting agencies? Yes

Does the law provide exceptions for entities complying with other laws?

HIPPA	Yes	**GLBA**	Yes	**Other:**	Yes

Does the law provide an exception if the entity maintains its own notification procedures? No

Does the law provide a private right of action for individuals? No

Source: https://codes.ohio.gov/ohio-revised-code/section-1349.19

Data Breach Notification Laws 2023

Oklahoma

24 Okla. Stat. tit. § 161—166

Effective: November 1, 2008

Definition of breach:

"Breach of the security of a system" means the unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of personal information maintained by an individual or entity as part of a database of personal information regarding multiple individuals and that causes, or the individual or entity reasonably believes has caused or will cause, identity theft or other fraud to any resident of this state; OKLA. STAT. tit. 24, § 162(1).

Definition of personally identifiable information:

"Personal information" means the first name or first initial and last name in combination with and linked to any one or more of the following data elements that relate to a resident of this state, when the data elements are neither encrypted nor redacted: social security number, driver license number or state identification card number issued in lieu of a driver license, or financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to the financial accounts of a resident; OKLA. STAT. tit. 24, § 162(6).

Does the definition of "personally identifiable information" or "breach" cover:

Biometric information:	No	**Medical information:**	No	**Passports and/or government IDs:**	Yes	**Paper records:**	No
De-identified information:	No	**Publicly available information:**	No	**Encrypted information:**	Yes	**Encrypted information when the encryption key was or is likely to have been exposed:**	Yes

Does the law cover?

Individuals:	Yes	**Businesses:**	Yes	**State government agencies:**	Yes

Notice Requirements:

Is there a "risk of harm" trigger for notification? Yes

What conditions allow for notice to be delayed?

The law allows for delays in notification under certain circumstances; OKLA. STAT. tit. 24, § 163(D).

If there are time limits for notification, how many days are permitted?

The law does not provide a specific number of days for notification, it states that the disclosure shall be made without unreasonable delay; OKLA. STAT. tit. 24, § 163(A).

Does the law specify how notice must be given? No

If yes, what must the notice include?

The law does not specify what information about the breach must be included in the data breach notification; OKLA. STAT. tit. 24, § 163.

Does the law permit notice by:

Mail:	Yes	**Email:**	Yes	**Website:**	Yes

Does the law require reporting to the State's Attorney General or a separate government agency under certain conditions? No

If a certain number of residents need to be affected for agency reporting, how many? N/A

Does agency share breach notifications? No

Does the law require reporting to consumer reporting agencies? No

Does the law provide exceptions for entities complying with other laws?

HIPPA	No	**GLBA**	Yes	**Other:**	Yes

Does the law provide an exception if the entity maintains its own notification procedures? Yes

Does the law provide a private right of action for individuals? No

Source: https://oklahoma.gov/content/dam/ok/en/orec/documents/archive/Security%20Breach%20Notification%20Act.pdf

Oregon

Or. Rev. Stat. §§ 646A.600 – 646A.604, 646A.624–646A.626

Effective: October 1, 2007

Definition of breach:

"Breach of security" means an unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of personal information that a person maintains or possesses; ORS 646A.602(1)(a).

Definition of personally identifiable information:

"Personal information" means a consumer's first name or first initial and last name in combination with any one or more of certain data elements, if encryption, redaction or other methods have not rendered the data elements unusable or if the data elements are encrypted and the encryption key has been acquired; ORS 646A.602(12)(a).

Does the definition of "personally identifiable information" or "breach" cover:

Biometric information:	Yes	**Medical information:**	Yes	**Passports and/or government IDs:**	Yes	**Paper records:**	No
De-identified information:	No	**Publicly available information:**	No	**Encrypted information:**	Yes	**Encrypted information when the encryption key was or is likely to have been exposed:**	Yes

Does the law cover?

Individuals:	Yes	**Businesses:**	Yes	**State government agencies:**	Yes

Notice Requirements:

Is there a "risk of harm" trigger for notification? Yes

What conditions allow for notice to be delayed?

There are permitted delays for notification if a law enforcement agency determines that a notification will impede a criminal investigation and if the law enforcement agency requests in writing that the covered entity delay the notification; ORS 646A.604(3)(c).

If there are time limits for notification, how many days are permitted?

The law provides a specific number of days permitted for notification once it is required. A covered entity shall give notice of a breach of security in the most expeditious manner possible, without unreasonable delay, but not later than 45 days after discovering or receiving notification of the breach of security; ORS 646A.604(3)(a).

Does the law specify how notice must be given? Yes

If yes, what must the notice include?

The law specifies what information about the breach must be included in the data breach notification; ORS 646A.604(5).

Does the law permit notice by:

Mail:	Yes	**Email:**	Yes	**Website:**	Yes

Does the law require reporting to the State's Attorney General or a separate government agency under certain conditions? Yes

If a certain number of residents need to be affected for agency reporting, how many? 1

Does agency share breach notifications? No

Does the law require reporting to consumer reporting agencies? Yes

Does the law provide exceptions for entities complying with other laws?

HIPPA	Yes	**GLBA**	Yes	**Other:**	Yes

Does the law provide an exception if the entity maintains its own notification procedures? No

Does the law provide a private right of action for individuals? No

Source: https://www.oregonlegislature.gov/bills_laws/ors/ors646A.html

Pennsylvania

73 Pa. Stat. §§ 2301–2308, 2329

Effective: June 20, 2006

Definition of breach:

"Breach of the security of the system" is defined as "The unauthorized access and acquisition of computerized data that materially compromises the security or confidentiality of personal information maintained by the entity as part of a database of personal information regarding multiple individuals and that causes or the entity reasonably believes has caused or will cause loss or injury to any resident of this Commonwealth."; 73 P.S. § 2302

Definition of personally identifiable information:

"Personal information" is defined as "An individual's first name or first initial and last name in combination with and linked to any one or more of the following data elements when the data elements are not encrypted or redacted: (i) Social Security number. (ii) Driver's license number or a State identification card number issued in lieu of a driver's license. (iii) Financial 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. (iv) Medical information. (v) Health insurance information. (vi) A user name or e-mail address, in combination with a password or security question and answer that would permit access to an online account."; 73 P.S. § 2302

Does the definition of "personally identifiable information" or "breach" cover:

Biometric information:	No	**Medical information:**	Yes	**Passports and/or government IDs:**	Yes	**Paper records:**	No
De-identified information:	No	**Publicly available information:**	No	**Encrypted information:**	Yes	**Encrypted information when the encryption key was or is likely to have been exposed:**	Yes

Does the law cover?

Individuals:	No	**Businesses:**	Yes	**State government agencies:**	Yes

Notice Requirements:

Is there a "risk of harm" trigger for notification? Yes

What conditions allow for notice to be delayed?

The law allows for permitted delays for notification if a law enforcement agency determines and advises the entity in writing that the notification will impede a criminal or civil investigation; 73 P.S. § 2304

If there are time limits for notification, how many days are permitted?

The law does not provide a specific number of days permitted for notification once it is required. It states that the notice shall be made without unreasonable delay; 73 P.S. § 2303(a)

Does the law specify how notice must be given? Yes

If yes, what must the notice include?

The law specifies what information about the breach must be included in the data breach notification. The notice must describe the incident in general terms and verify personal information but does not require the individual to provide personal information; 73 P.S. § 2302

Does the law permit notice by:

Mail:	Yes	**Email:**	Yes	**Website:**	Yes

Does the law require reporting to the State's Attorney General or a separate government agency under certain conditions? Yes

If a certain number of residents need to be affected for agency reporting, how many? 1

Does agency share breach notifications? No

Does the law require reporting to consumer reporting agencies? Yes

Does the law provide exceptions for entities complying with other laws?

HIPPA	Yes	**GLBA**	No	**Other:**	Yes

Does the law provide an exception if the entity maintains its own notification procedures? Yes

Does the law provide a private right of action for individuals? No

Source:

https://govt.westlaw.com/pac/Browse/Home/Pennsylvania/UnofficialPurdonsPennsylvaniaStatutes?guid=N9B3F41908C4F11DA86FC8D90DD1949D4&originationContext=documenttoc&transitionType=Default&contextData=(sc.Default)

Rhode Island

R.I. Gen Laws §§ 11-49.3-2—11-49.3-6

Effective: July, 2016

Definition of breach:

"Breach of the security of the system" means unauthorized access or acquisition of unencrypted, computerized data information that compromises the security, confidentiality, or integrity of personal information maintained by the municipal agency, state agency, or person. Good-faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency is not a breach of the security of the system; provided, that the personal information is not used or subject to further unauthorized disclosure; § 11-49.3-3(a)(1).

Definition of personally identifiable information:

"Personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when the name and the data elements are not encrypted or are in hard copy, paper format: Social security number; Driver's license number, Rhode Island identification card number, or tribal identification number; Account number, credit, or debit card number, in combination with any required security code, access code, password, or personal identification number, that would permit access to an individual's financial account; Medical or health insurance information; or E-mail address with any required security code, access code, or password that would permit access to an individual's personal, medical, insurance, or financial account; § 11-49.3-3(a)(8).

Does the definition of "personally identifiable information" or "breach" cover:

Biometric information:	No	**Medical information:**	Yes	**Passports and/or government IDs:**	Yes	**Paper records:**	Yes
De-identified information:	No	**Publicly available information:**	No	**Encrypted information:**	No	**Encrypted information when the encryption key was or is likely to have been exposed:**	No

Does the law cover?

Individuals:	Yes	**Businesses:**	Yes	**State government agencies:**	Yes

Notice Requirements:

Is there a "risk of harm" trigger for notification? Yes

What conditions allow for notice to be delayed?

The notification required by this section may be delayed if a federal, state, or local law enforcement agency determines that the notification will impede a criminal investigation; § 11-49.3-4(b).

If there are time limits for notification, how many days are permitted?

The notification shall be made in the most expedient time possible, but no later than forty-five (45) calendar days after confirmation of the breach; § 11-49.3-4(a)(2).

Does the law specify how notice must be given? Yes

If yes, what must the notice include?

The notification to individuals must include a general and brief description of the incident, the type of information that was subject to the breach, date of breach, date that the breach was discovered, a description of any remediation services offered to affected individuals, and a description of the consumer's ability to file or obtain a police report; § 11-49.3-4(d).

Does the law permit notice by:

Mail:	Yes	**Email:**	Yes	**Website:**	Yes

Does the law require reporting to the State's Attorney General or a separate government agency under certain conditions? Yes

If a certain number of residents need to be affected for agency reporting, how many? 500

Does agency share breach notifications? No

Does the law require reporting to consumer reporting agencies? Yes

Does the law provide exceptions for entities complying with other laws?

HIPPA	Yes	**GLBA**	Yes	**Other:**	Yes

Does the law provide an exception if the entity maintains its own notification procedures? Yes

Does the law provide a private right of action for individuals? No

Source: http://webserver.rilin.state.ri.us/Statutes/TITLE11/11-49.3/INDEX.HTM

South Carolina

S.C. Code. § 39-1-90

Effective: July 1, 2009

Definition of breach:

"Breach of the security of the system" means unauthorized access to and acquisition of computerized data that was not rendered unusable through encryption, redaction, or other methods that compromises the security, confidentiality, or integrity of personal identifying information maintained by the person, when illegal use of the information has occurred or is reasonably likely to occur or use of the information creates a material risk of harm to a resident; SECTION 39-1-90(D)(1).

Definition of personally identifiable information:

"Personal identifying information" means the first name or first initial and last name in combination with and linked to any one or more of the following data elements that relate to a resident of this State, when the data elements are neither encrypted nor redacted: social security number; driver's license number or state identification card number issued instead of a driver's license; financial account number, or credit card or debit card number in combination with any required security code, access code, or password that would permit access to a resident's financial account; or 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 uniquely will identify an individual; SECTION 39-1-90(D)(3).

Does the definition of "personally identifiable information" or "breach" cover:

Biometric information:	No	**Medical information:**	No	**Passports and/or government IDs:**	Yes	**Paper records:**	No
De-identified information:	No	**Publicly available information:**	No	**Encrypted information:**	No	**Encrypted information when the encryption key was or is likely to have been exposed:**	Yes

Does the law cover?

Individuals:	Yes	**Businesses:**	Yes	**State government agencies:**	No

Notice Requirements:

Is there a "risk of harm" trigger for notification? Yes

What conditions allow for notice to be delayed?

The law allows for delays in notification if a law enforcement agency determines that the notification impedes a criminal investigation; SECTION 39-1-90(C).

If there are time limits for notification, how many days are permitted?

The law does not provide a specific number of days for notification, only stating that it must be made in the most expedient time possible and without unreasonable delay; SECTION 39-1-90(A).

Does the law specify how notice must be given? No

If yes, what must the notice include?

The law does not specify what information about the breach must be included in the data breach notification; SECTION 39-1-90.

Does the law permit notice by:

Mail:	Yes	**Email:**	Yes	**Website:**	Yes

Does the law require reporting to the State's Attorney General or a separate government agency under certain conditions? Yes

If a certain number of residents need to be affected for agency reporting, how many? 1000

Does agency share breach notifications? No

Does the law require reporting to consumer reporting agencies? Yes

Does the law provide exceptions for entities complying with other laws?

HIPPA	No	**GLBA**	Yes	**Other:**	Yes

Does the law provide an exception if the entity maintains its own notification procedures? Yes

Does the law provide a private right of action for individuals? Yes

Source: https://www.scstatehouse.gov/code/t39c001.php

South Dakota

S.D. Code §§ 22-40-19—22-40-26

Effective: July 1, 2018

Definition of breach:

"Breach of system security," means the unauthorized acquisition of unencrypted computerized data or encrypted computerized data and the encryption key by any person that materially compromises the security, confidentiality, or integrity of personal or protected information maintained by the information holder. The term does not include the good faith acquisition of personal or protected information by an employee or agent of the information holder for the purposes of the information holder if the personal or protected information is not used or subject to further unauthorized disclosure; SDCL § 22-40-19(1).

Definition of personally identifiable information:

"Personal information," means a person's first name or first initial and last name, in combination with any one or more of the following data elements: Social security number; Driver license number or other unique identification number created or collected by a government body; Account, credit card, or debit card number, in combination with any required security code, access code, password, routing number, PIN, or any additional information that would permit access to a person's financial account; Health information as defined in 45 CFR 160.103; or An identification number assigned to a person by the person's employer in combination with any required security code, access code, password, or biometric data generated from measurements or analysis of human body characteristics for authentication purposes. The term does not include information that is lawfully made available to the general public from federal, state, or local government records or information that has been redacted, or otherwise made unusable; SDCL § 22-40-19(4).

Does the definition of “personally identifiable information” or “breach” cover:

Biometric information:	Yes	**Medical information:**	Yes	**Passports and/or government IDs:**	Yes	**Paper records:**	No
De-identified information:	No	**Publicly available information:**	No	**Encrypted information:**	Yes	**Encrypted information when the encryption key was or is likely to have been exposed:**	Yes

Does the law cover?

Individuals:	Yes	**Businesses:**	Yes	**State government agencies:**	Yes

Notice Requirements:

Is there a "risk of harm" trigger for notification? Yes

What conditions allow for notice to be delayed?

The law allows for delays in notification if required by law enforcement or if the information holder determines that the breach will not likely result in harm to the affected person; SDCL § 22-40-20, SDCL § 22-40-21.

If there are time limits for notification, how many days are permitted?

A disclosure under this section shall be made not later than sixty days from the discovery or notification of the breach of system security; SDCL § 22-40-20.

Does the law specify how notice must be given? No

If yes, what must the notice include?

The law does not specify what information about the breach must be included in the data breach notification; SDCL § 22-40-22.

Does the law permit notice by:

Mail:	Yes	**Email:**	Yes	**Website:**	Yes

Does the law require reporting to the State's Attorney General or a separate government agency under certain conditions? Yes

If a certain number of residents need to be affected for agency reporting, how many? 250

Does agency share breach notifications? No

Does the law require reporting to consumer reporting agencies? Yes

Does the law provide exceptions for entities complying with other laws?

HIPPA	Yes	**GLBA**	Yes	**Other:**	Yes

Does the law provide an exception if the entity maintains its own notification procedures? Yes

Does the law provide a private right of action for individuals? No

Source: https://sdlegislature.gov/Statutes/Codified_Laws/2047702

Data Breach Notification Laws 2023

Tennessee

Tenn. Code §§ 47-18-2105—47-18-2107

Effective: July 1, 2005

Definition of breach:

"Breach of system security" means the acquisition of unencrypted computerized data or encrypted computerized data and the encryption key by an unauthorized person that materially compromises the security, confidentiality, or integrity of personal information maintained by the information holder; TENN. CODE ANN. § 47-18-2107(a)(1).

Definition of personally identifiable information:

"Personal information" means an individual's first name or first initial and last name, in combination with any one or more of the following data elements: Social security number; Driver license number; or Account, credit card, 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; TENN. CODE ANN. § 47-18-2107(a)(4).

Does the definition of "personally identifiable information" or "breach" cover:

Biometric information:	No	**Medical information:**	No	**Passports and/or government IDs:**	Yes	**Paper records:**	No
De-identified information:	No	**Publicly available information:**	No	**Encrypted information:**	Yes	**Encrypted information when the encryption key was or is likely to have been exposed:**	Yes

Does the law cover?

Individuals:	No	**Businesses:**	Yes	**State government agencies:**	Yes

Notice Requirements:

Is there a "risk of harm" trigger for notification? No

What conditions allow for notice to be delayed?

The law allows for delays in notification due to the legitimate needs of law enforcement; TENN. CODE ANN. § 47-18-2107(d).

If there are time limits for notification, how many days are permitted?

The law specifies that the disclosure must be made no later than forty-five (45) days from the discovery or notification of the breach of system security; TENN. CODE ANN. § 47-18-2107(b).

Does the law specify how notice must be given? No

If yes, what must the notice include?

The law does not specify what information about the breach must be included in the data breach notification; TENN. CODE ANN. § 47-18-2107.

Does the law permit notice by:

Mail:	Yes	**Email:**	Yes	**Website:**	Yes

Does the law require reporting to the State's Attorney General or a separate government agency under certain conditions? No

If a certain number of residents need to be affected for agency reporting, how many? N/A

Does agency share breach notifications? No

Does the law require reporting to consumer reporting agencies? Yes

Does the law provide exceptions for entities complying with other laws?

HIPPA	Yes	**GLBA**	Yes	**Other:**	No

Does the law provide an exception if the entity maintains its own notification procedures? Yes

Does the law provide a private right of action for individuals? Yes

Source: https://advance.lexis.com/documentpage/?pdmfid=1000516&crid=276bded8-ea5d-427c-8661-5cb10d673b62&nodeid=ABVAAUAAVAAH&nodepath=%2fROOT%2fABV%2fABVAAU%2fABVAAUAAV%2fABVAAUAAVAAH&level=4&haschildren=&populated=false&title=47-18-2107.+Release+of+personal+consumer+information.&config=025054JABlOTJjNmIyNi0wYjI0LTRjZGEtYWE5ZC0zNGFhOWNhMjFlNDgKAFBvZENhdGFsb2cDFQ14bX2GfyBTaI9WcPX5&pddocfullpath=%2fshared%2fdocument%2fstatutes-legislation%2furn%3acontentItem%3a4X8K-XB40-R03J-K1K5-00008-00&ecomp=f38_kkk&prid=ae167118-3d03-4a8c-af3c-83c6191bfd5e

Data Breach Notification Laws 2023

Texas

Tex. Bus. & Com. Code §§ 521.002, 521.053, 521.151

Effective: April 1, 2009

Definition of breach:

"'Breach of system security' means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information maintained by a person, including data that is encrypted if the person accessing the data has the key required to decrypt the data. Good faith acquisition of sensitive personal information by an employee or agent of the person for the purposes of the person is not a breach of system security unless the person uses or discloses the sensitive personal information in an unauthorized manner; TEX. BUS. & COM. CODE § 521.053(a)"

Definition of personally identifiable information:

"'Personal identifying information' means information that alone or in conjunction with other information identifies an individual, including an individual's name, social security number, date of birth, or government-issued identification number, mother's maiden name, unique biometric data, unique electronic identification number, address, or routing code, and telecommunication access device. 'Sensitive personal information' means an individual's first name or first initial and last name in combination with any one or more of the following items, if the name and the items are not encrypted: social security number; driver's license number or government-issued identification number; or account number or 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; or information that identifies an individual and relates to the physical or mental health or condition of the individual, the provision of health care to the individual, or payment for the provision of health care to the individual; TEX. BUS. & COM. CODE § 521.002(a)(1)(2)"

Does the definition of "personally identifiable information" or "breach" cover:

Biometric information:	Yes	**Medical information:**	Yes	**Passports and/or government IDs:**	Yes	**Paper records:**	No
De-identified information:	No	**Publicly available information:**	No	**Encrypted information:**	Yes	**Encrypted information when the encryption key was or is likely to have been exposed:**	Yes

Does the law cover?

Individuals:	Yes	**Businesses:**	Yes	**State government agencies:**	No

Notice Requirements:

Is there a "risk of harm" trigger for notification? No

What conditions allow for notice to be delayed?

A person may delay providing notice at the request of a law enforcement agency that determines that the notification will impede a criminal investigation; TEX. BUS. & COM. CODE § 521.053(d)"

If there are time limits for notification, how many days are permitted?

The disclosure shall be made without unreasonable delay and in each case not later than the 60th day after the date on which the person determines that the breach occurred; TEX. BUS. & COM. CODE § 521.053(b)"

Does the law specify how notice must be given? Yes

If yes, what must the notice include?

The notification to the attorney general must include a detailed description of the nature and circumstances of the breach or the use of sensitive personal information acquired as a result of the breach; TEX. BUS. & COM. CODE § 521.053(i)(1)"

Does the law permit notice by:

Mail:	Yes	**Email:**	Yes	**Website:**	Yes

Does the law require reporting to the State's Attorney General or a separate government agency under certain conditions? Yes

If a certain number of residents need to be affected for agency reporting, how many? 250

Does agency share breach notifications? Yes

Does the law require reporting to consumer reporting agencies? Yes

Does the law provide exceptions for entities complying with other laws?

HIPPA	No	**GLBA**	No	**Other:**	No

Does the law provide an exception if the entity maintains its own notification procedures? Yes

Does the law provide a private right of action for individuals? No

Source: https://statutes.capitol.texas.gov/Docs/BC/htm/BC.521.htm#521.002

Data Breach Notification Laws 2023

Utah

Utah Code §§ 13-44-101—13-44-301

Effective: January 1, 2007

Definition of breach:

"Breach of system security" means an unauthorized acquisition of computerized data maintained by a person that compromises the security, confidentiality, or integrity of personal information. It does not include the acquisition of personal information by an employee or agent of the person possessing unencrypted computerized data unless the personal information is used for an unlawful purpose or disclosed in an unauthorized manner; UTAH CODE ANN. § 13-44-102(1).

Definition of personally identifiable information:

"Personal information" means a person's first name or first initial and last name, combined with any one or more of the following data elements relating to that person when either the name or date element is unencrypted or not protected by another method that renders the data unreadable or unusable: (i) Social Security number; (ii) (A) financial account number, or credit or debit card number; and (B) any required security code, access code, or password that would permit access to the person's account; or (iii) driver license number or state identification card number; UTAH CODE ANN. § 13-44-102(4).

Does the definition of "personally identifiable information" or "breach" cover:

Biometric information:	No	**Medical information:**	No	**Passports and/or government IDs:**	Yes	**Paper records:**	Yes
De-identified information:	No	**Publicly available information:**	No	**Encrypted information:**	No	**Encrypted information when the encryption key was or is likely to have been exposed:**	No

Does the law cover?

Individuals:	Yes	**Businesses:**	Yes	**State government agencies:**	No

Notice Requirements:

Is there a "risk of harm" trigger for notification? Yes

What conditions allow for notice to be delayed?

A person may delay providing notification at the request of a law enforcement agency that determines that notification may impede a criminal investigation; UTAH CODE ANN. § 13-44-202(4)(a).

If there are time limits for notification, how many days are permitted?

The law does not provide a specific number of days permitted for notification once it is required. It states that notification should be provided in the most expedient time possible without unreasonable delay; UTAH CODE ANN. § 13-44-202(2).

Does the law specify how notice must be given? No

If yes, what must the notice include?

The law does not explicitly specify what information about the breach must be included in the data breach notification; UTAH CODE ANN. § 13-44-202.

Does the law permit notice by:

Mail:	Yes	**Email:**	Yes	**Website:**	No

Does the law require reporting to the State's Attorney General or a separate government agency under certain conditions? Yes

If a certain number of residents need to be affected for agency reporting, how many? 500

Does agency share breach notifications? No

Does the law require reporting to consumer reporting agencies? Yes

Does the law provide exceptions for entities complying with other laws?

HIPPA	No	**GLBA**	No	**Other:**	Yes

Does the law provide an exception if the entity maintains its own notification procedures? Yes

Does the law provide a private right of action for individuals? No

Source: https://le.utah.gov/xcode/Title13/Chapter44/13-44.html?v=C13-44_1800010118000101

Data Breach Notification Laws 2023

Vermont

9 V.S.A §§ 2430, 2435

Effective: May 8, 2012

Definition of breach:

"'Security breach' means unauthorized acquisition of electronic data, or a reasonable belief of an unauthorized acquisition of electronic data, that compromises the security, confidentiality, or integrity of a consumer's personally identifiable information or login credentials maintained by a data collector; VT. STAT. ANN. tit. 9, § 2430(13)(A)

Definition of personally identifiable information:

"'Personally identifiable information' means a consumer's first name or first initial and last name in combination with one or more of the following digital data elements, when the data elements are not encrypted, redacted, or protected by another method that renders them unreadable or unusable by unauthorized persons; VT. STAT. ANN. tit. 9, § 2430(10)(A)

Does the definition of "personally identifiable information" or "breach" cover:

Biometric information:	Yes	**Medical information:**	Yes	**Passports and/or government IDs:**	Yes	**Paper records:**	Yes
De-identified information:	No	**Publicly available information:**	No	**Encrypted information:**	Yes	**Encrypted information when the encryption key was or is likely to have been exposed:**	Yes

Does the law cover?

Individuals:	Yes	**Businesses:**	Yes	**State government agencies:**	Yes

Notice Requirements:

Is there a "risk of harm" trigger for notification? Yes

What conditions allow for notice to be delayed?

There are permitted delays for notification. The law allows for delay of notification upon request of a law enforcement agency; VT. STAT. ANN. tit. 9, § 2435(b)(4)(A)

If there are time limits for notification, how many days are permitted?

The law provides a specific number of days permitted for notification once it is required. Notification must be made 'not later than 45 days after the discovery or notification'; VT. STAT. ANN. tit. 9, § 2435(b)(1)

Does the law specify how notice must be given? Yes

If yes, what must the notice include?

The law specifies what information about the breach must be included in the data breach notification. The notice to a consumer of a security breach involving personally identifiable information shall include a description of the incident in general terms, the type of personally identifiable information that was subject to the security breach, the general acts of the data collector to protect the personally identifiable information from further security breach, a telephone number that the consumer may call for further information and assistance, advice that directs the consumer to remain vigilant by reviewing account statements and monitoring free credit reports, and the approximate date of the security breach; VT. STAT. ANN. tit. 9, § 2435(b)(5)

Does the law permit notice by:

Mail:	Yes	**Email:**	Yes	**Website:**	Yes

Does the law require reporting to the State's Attorney General or a separate government agency under certain conditions? Yes

If a certain number of residents need to be affected for agency reporting, how many? 1

Does agency share breach notifications? No

Does the law require reporting to consumer reporting agencies? Yes

Does the law provide exceptions for entities complying with other laws?

HIPPA	Yes	**GLBA**	No	**Other:**	No

Does the law provide an exception if the entity maintains its own notification procedures? No

Does the law provide a private right of action for individuals? No

Source: https://legislature.vermont.gov/statutes/chapter/09/062

Data Breach Notification Laws 2023

Virginia

Va. Code §§ 18.2—186.6; 32.1-127.1:05

Effective: July 1, 2008

Definition of breach:

"Breach of the security of the system" means the unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of personal information maintained by an individual or entity as part of a database of personal information regarding multiple individuals and that causes, or the individual or entity reasonably believes has caused, or will cause, identity theft or other fraud to any resident of the Commonwealth; VA. CODE ANN. § 18.2-186.6(A).

Definition of personally identifiable information:

"Personal information" means the first name or first initial and last name in combination with and linked to any one or more of the following data elements that relate to a resident of the Commonwealth, when the data elements are neither encrypted nor redacted: Social security number; Driver's license number or state identification card number issued in lieu of a driver's license number; Financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial accounts; Passport number; or Military identification number; VA. CODE ANN. § 18.2-186.6(A).

Does the definition of “personally identifiable information” or “breach” cover:

Biometric information:	No	**Medical information:**	No	**Passports and/or government IDs:**	Yes	**Paper records:**	No
De-identified information:	No	**Publicly available information:**	No	**Encrypted information:**	Yes	**Encrypted information when the encryption key was or is likely to have been exposed:**	Yes

Does the law cover?

Individuals:	Yes	**Businesses:**	Yes	**State government agencies:**	Yes

Notice Requirements:

Is there a “risk of harm” trigger for notification? Yes

What conditions allow for notice to be delayed?

The law allows for reasonable delays in notification under certain circumstances; VA. CODE ANN. § 18.2-186.6(B).

If there are time limits for notification, how many days are permitted?

The law does not provide a specific number of days for notification, but requires it to be done without unreasonable delay; VA. CODE ANN. § 18.2-186.6(B).

Does the law specify how notice must be given? Yes

If yes, what must the notice include?

The law specifies that the notice should include a description of the incident, the type of personal information that was subject to the unauthorized access and acquisition, the general acts of the individual or entity to protect the personal information from further unauthorized access, a telephone number for further information and assistance, and advice to remain vigilant by reviewing account statements and monitoring free credit reports; VA. CODE ANN. § 18.2-186.6(A).

Does the law permit notice by:

Mail:	Yes	**Email:**	Yes	**Website:**	Yes

Does the law require reporting to the State's Attorney General or a separate government agency under certain conditions? Yes

If a certain number of residents need to be affected for agency reporting, how many? 1

Does agency share breach notifications? No

Does the law require reporting to consumer reporting agencies? Yes

Does the law provide exceptions for entities complying with other laws?

HIPPA	No	**GLBA**	Yes	**Other:**	Yes

Does the law provide an exception if the entity maintains its own notification procedures? Yes

Does the law provide a private right of action for individuals? No

Source: https://law.lis.virginia.gov/vacode/title18.2/chapter6/section18.2-186.6/

Washington

Wash. Rev. Code §§ 19.255.005—19.255.020; 42.56.590

Effective: July 24, 2005

Definition of breach:

"Breach of the security of the system" means unauthorized acquisition of data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system when the personal information is not used or subject to further unauthorized disclosure; Washington State Data Breach Notification Law Section 1.

Definition of personally identifiable information:

"Personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements: Social security number; Driver's license number or Washington identification card number; Account number or 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, or any other numbers or information that can be used to access a person's financial account; Full date of birth; Private key that is unique to an individual and that is used to authenticate or sign an electronic record; Student, military, or passport identification number; Health insurance policy number or health insurance identification number; 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; or Biometric data generated by automatic measurements of an individual's biological characteristics such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual; User name or email address in combination with a password or security questions and answers that would permit access to an online account; and Any of the data elements or any combination of the data elements described in this subsection without the consumer's first name or first initial and last name if encryption, redaction, or other methods have not rendered the data element or combination of data elements unusable; and The data element or combination of data elements would enable a person to commit identity theft against a consumer; Washington State Data Breach Notification Law Section 2(a).

Does the definition of "personally identifiable information" or "breach" cover:

Biometric information:	Yes	**Medical information:**	Yes	**Passports and/or government IDs:**	Yes	**Paper records:**	No
De-identified information:	No	**Publicly available information:**	No	**Encrypted information:**	Yes	**Encrypted information when the encryption key was or is likely to have been exposed:**	Yes

Does the law cover?

Individuals:	Yes	**Businesses:**	Yes	**State government agencies:**	No

Notice Requirements:

Is there a "risk of harm" trigger for notification? Yes

What conditions allow for notice to be delayed?

The notification required by this section may be delayed if the data owner or licensee contacts a law enforcement agency after discovery of a breach of the security of the system and a law enforcement agency determines that the notification will impede a criminal investigation; Washington State Data Breach Notification Law Section 3.

If there are time limits for notification, how many days are permitted?

Notification to affected consumers under this section must be made in the most expedient time possible, without unreasonable delay, and no more than thirty calendar days after the breach was discovered; Washington State Data Breach Notification Law Section 8.

Does the law specify how notice must be given? Yes

If yes, what must the notice include?

The notification must include, at a minimum, the following information: The name and contact information of the reporting person or business subject to this section; A list of the types of personal information that were or are reasonably believed to have been the subject of a breach; A time frame of exposure, if known, including the date of the breach and the date of the discovery of the breach; and The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed personal information; Washington State Data Breach Notification Law Section 6(b).

Does the law permit notice by:

Mail:	Yes	**Email:**	Yes	**Website:**	Yes

Does the law require reporting to the State's Attorney General or a separate government agency under certain conditions? Yes

If a certain number of residents need to be affected for agency reporting, how many? 500

Does agency share breach notifications? No

Does the law require reporting to consumer reporting agencies? No

Does the law provide exceptions for entities complying with other laws?

HIPPA	No	**GLBA**	No	**Other:**	No

Does the law provide an exception if the entity maintains its own notification procedures? Yes

Does the law provide a private right of action for individuals? No

Source: https://apps.leg.wa.gov/RCW/default.aspx?cite=19.255.010

West Virginia

W. Va. Code §§ 46A-2A-101—46A-2A-105

Effective: June 6, 2008

Definition of breach:

"'Breach of the security of a system' means the unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of personal information maintained by an individual or entity as part of a database of personal information regarding multiple individuals and that causes the individual or entity to reasonably believe that the breach of security has caused or will cause identity theft or other fraud to any resident of this state. Good faith acquisition of personal information by an employee or agent of an individual or entity for the purposes of the individual or the entity is not a breach of the security of the system, provided that the personal information is not used for a purpose other than a lawful purpose of the individual or entity or subject to further unauthorized disclosure; §46A-2A-101(1)."

Definition of personally identifiable information:

"'Personal information' means the first name or first initial and last name linked to any one or more of the following data elements that relate to a resident of this state, when the data elements are neither encrypted nor redacted: (A) Social security number; (B) Driver's license number or state identification card number issued in lieu of a driver's license; or (C) Financial account number, or credit card, or debit card number in combination with any required security code, access code or password that would permit access to a resident's financial accounts; §46A-2A-101(6)."

Does the definition of "personally identifiable information" or "breach" cover:

Biometric information:	No	**Medical information:**	No	**Passports and/or government IDs:**	Yes	**Paper records:**	No
De-identified information:	No	**Publicly available information:**	No	**Encrypted information:**	No	**Encrypted information when the encryption key was or is likely to have been exposed:**	Yes

Does the law cover?

Individuals:	Yes	**Businesses:**	Yes	**State government agencies:**	Yes

Notice Requirements:

Is there a "risk of harm" trigger for notification? Yes

What conditions allow for notice to be delayed?

The law allows for permitted delays for notification if a law-enforcement agency determines and advises the individual or entity that the notice will impede a criminal or civil investigation or homeland or national security; §46A-2A-102(e)."

If there are time limits for notification, how many days are permitted?

The law does not provide a specific number of days permitted for notification once it is required. It mentions that the notice shall be made without unreasonable delay; §46A-2A-102(a)."

Does the law specify how notice must be given? Yes

If yes, what must the notice include?

The law specifies what information about the breach must be included in the data breach notification; §46A-2A-102(d)."

Does the law permit notice by:

Mail:	Yes	**Email:**	Yes	**Website:**	Yes

Does the law require reporting to the State's Attorney General or a separate government agency under certain conditions? No

If a certain number of residents need to be affected for agency reporting, how many? N/A

Does agency share breach notifications? No

Does the law require reporting to consumer reporting agencies? Yes

Does the law provide exceptions for entities complying with other laws?

HIPPA	No	**GLBA**	No	**Other:**	Yes

Does the law provide an exception if the entity maintains its own notification procedures? Yes

Does the law provide a private right of action for individuals? No

Source: http://www.wvlegislature.gov/WVCODE/Code.cfm?chap=46a&art=2A#2A

Wisconsin

Wis. Stat. § 134.98

Effective: March 31, 2006

Definition of breach:

"Breach" is defined as the unauthorized acquisition of personal information by a person whom the entity has not authorized to acquire the personal information; WIS. STAT. § 134.98(2)(a).

Definition of personally identifiable information:

"Personally Identifiable Information" is defined as an individual's last name and the individual's first name or first initial, in combination with and linked to any of the following elements, if the element is not publicly available information and is not encrypted, redacted, or altered in a manner that renders the element unreadable: The individual's social security number, driver's license number or state identification number, financial account number, deoxyribonucleic acid profile, or unique biometric data; WIS. STAT. § 134.98(1)(b).

Does the definition of "personally identifiable information" or "breach" cover:

Biometric information:	Yes	**Medical information:**	No	**Passports and/or government IDs:**	Yes	**Paper records:**	No
De-identified information:	No	**Publicly available information:**	No	**Encrypted information:**	No	**Encrypted information when the encryption key was or is likely to have been exposed:**	No

Does the law cover?

Individuals:	No	**Businesses:**	Yes	**State government agencies:**	Yes

Notice Requirements:

Is there a "risk of harm" trigger for notification? Yes

What conditions allow for notice to be delayed?

There are permitted delays for notification if a law enforcement agency asks an entity not to provide a notice that is otherwise required under sub. (2) for any period of time; WIS. STAT. § 134.98(5).

If there are time limits for notification, how many days are permitted?

The law provides a specific number of days permitted for notification once it is required, which is within a reasonable time, not to exceed 45 days after the entity learns of the acquisition of personal information; WIS. STAT. § 134.98(3)(a).

Does the law specify how notice must be given? Yes

If yes, what must the notice include?

The law specifies that the notice shall indicate that the entity knows of the unauthorized acquisition of personal information pertaining to the subject of the personal information; WIS. STAT. § 134.98(2)(a).

Does the law permit notice by:

Mail:	Yes	**Email:**	No	**Website:**	No

Does the law require reporting to the State's Attorney General or a separate government agency under certain conditions? No

If a certain number of residents need to be affected for agency reporting, how many? N/A

Does agency share breach notifications? No

Does the law require reporting to consumer reporting agencies? Yes

Does the law provide exceptions for entities complying with other laws?

HIPPA	Yes	**GLBA**	Yes	**Other:**	No

Does the law provide an exception if the entity maintains its own notification procedures? No

Does the law provide a private right of action for individuals? No

Source: https://docs.legis.wisconsin.gov/statutes/statutes/134/98

Data Breach Notification Laws 2023

Wyoming

Wyo. Stat. §§ 40-12-501—40-12-509.

Effective: July 1, 2007

Definition of breach:

"Breach of the security of the data system" means unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of personal identifying information maintained by a person or business and causes or is reasonably believed to cause loss or injury to a resident of this state. Good faith acquisition of personal identifying information by an employee or agent of a person or business for the purposes of the person or business is not a breach of the security of the data system, provided that the personal identifying information is not used or subject to further unauthorized disclosure; WYO. STAT. ANN. § 40-12-501(a)(i)

Definition of personally identifiable information:

"Personal identifying information" means the first name or first initial and last name of a person in combination with one (1) or more of the data elements specified in W.S. 6-3-901(b)(iii) through (xiv), when the data elements are not redacted; WYO. STAT. ANN. § 40-12-501(a)(vii)

Does the definition of "personally identifiable information" or "breach" cover:

Biometric information:	No	**Medical information:**	No	**Passports and/or government IDs:**	Yes	**Paper records:**	No
De-identified information:	No	**Publicly available information:**	No	**Encrypted information:**	No	**Encrypted information when the encryption key was or is likely to have been exposed:**	No

Does the law cover?

Individuals:	Yes	**Businesses:**	Yes	**State government agencies:**	No

Notice Requirements:

Is there a "risk of harm" trigger for notification? Yes

What conditions allow for notice to be delayed?

The notification required by this section may be delayed if a law enforcement agency determines in writing that the notification may seriously impede a criminal investigation; WYO. STAT. ANN. § 40-12-502(b)

If there are time limits for notification, how many days are permitted?

The law states that notice shall be made in the most expedient time possible and without unreasonable delay, but does not provide a specific number of days; WYO. STAT. ANN. § 40-12-502(a)

Does the law specify how notice must be given? Yes

If yes, what must the notice include?

Notice required under subsection (a) of this section shall be clear and conspicuous and shall include, at a minimum, the types of personal identifying information that were or are reasonably believed to have been the subject of the breach, a general description of the breach incident, the approximate date of the breach of security, if that information is reasonably possible to determine at the time notice is provided, in general terms, the actions taken by the individual or commercial entity to protect the system containing the personal identifying information from further breaches, advice that directs the person to remain vigilant by reviewing account statements and monitoring credit reports, and whether notification was delayed as a result of a law enforcement investigation, if that information is reasonably possible to determine at the time the notice is provided; WYO. STAT. ANN. § 40-12-502(e)

Does the law permit notice by:

Mail:	Yes	**Email:**	Yes	**Website:**	Yes

Does the law require reporting to the State's Attorney General or a separate government agency under certain conditions? No

If a certain number of residents need to be affected for agency reporting, how many? N/A

Does agency share breach notifications? No

Does the law require reporting to consumer reporting agencies? No

Does the law provide exceptions for entities complying with other laws?

HIPPA	No	**GLBA**	Yes	**Other:**	Yes

Does the law provide an exception if the entity maintains its own notification procedures? No

Does the law provide a private right of action for individuals? No

Source: https://wyoleg.gov/statutes/compress/title40.pdf