CSR®
Privacy Made Simple℠

State of Virginia

Statutory Review for Breach & Consumer Notification

This summary of regulations is provided for information purposes only. No action based on this summary alone should be undertaken. Each individual or entity must obtain appropriate guidance for its specific circumstances.

48 states and the District of Columbia (Washington DC) have laws pertaining to the way they expect a breach to be handled and how they want their affected residents to be notified. If you have customers or have personal information pertaining to individuals that reside outside of your state, you will additionally need to ensure that you follow the laws of that corresponding state or country.

Following is a brief review of the Virginia laws pertaining to breach and consumer notification.

Personal Information
There is specific personal information that the state considers relevant to a breach. (This does not include elements that a federal agency or industry specific entity may consider relevant.)
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: a) Social security number; b) Driver's license number or state identification card number; or c) Financial account number, 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. In addition, there is a statute for Breach of Medical Information. Medical 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: a) Any information regarding an individual's medical or mental health history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or b) An individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.

CSR®
Privacy Made Simple℠

Who does the law apply to?
The state will identify who the law pertains to. The state may have different laws for state agencies or specialized fields such as medical or financial.
The law applies to an individual or entity that owns or licenses computerized data that includes personal information (data owner). "Entity" includes corporations, business trusts, estates, partnerships, limited partnerships, limited liability partnerships, limited liability companies, associations, organizations, joint ventures, governments, governmental subdivisions, agencies, or instrumentalities or any other legal entity, whether for profit or not for profit. In relation to medical breaches, "Entity" means any authority, board, bureau, commission, district or agency of the Commonwealth or of any political subdivision of the Commonwealth, including cities, towns and counties, municipal councils, governing bodies of counties, school boards and planning commissions; boards of visitors of public institutions of higher education; and other organizations, corporations, or agencies in the Commonwealth supported wholly or principally by public funds. Additionally, it applies to an individual or entity that maintains computerized data that includes personal information that the individual or entity does not own or license (vendor). If the vendor experiences a breach of security, they must notify the data owner without unreasonable delay. The data owner is responsible to complete the reporting and consumer notification. There are exceptions for entities under federal regulations, but minimum standards must be met.
Breach
There are many factors to take into consideration when deciding if the incident is considered a breach and when that breach is reportable. Some states have very specific factors while others leave the interpretation open to include a multitude of elements.
In Virginia, "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. When considering reporting requirements, it would include, but not be limited to: • The combination of personal information breached; • If the data was computerized; • If the data was encrypted, redacted, or otherwise altered; • If the data included any kind of key, access code or cipher; • If encrypted information was accessed and acquired in an unencrypted form; • If it was acquired by an unauthorized person; or • If it may be used for identity theft or other fraud.

Breach Reporting
There may be specific time limits to report a breach and complete consumer notification. There may be specific entities to report to.
The notification may be delayed if, after the individual or entity notifies a law-enforcement agency, the law-enforcement agency determines and advises them that the notice will impede a criminal or civil investigation, or homeland or national security. Notice must be made to the state attorney general and any affected resident without unreasonable delay. The notice must include specific comprehensive information such as the description of the incident, the type of personal information that was obtained, etc. For medical breaches, notice must also be given to the Commissioner of Health. If more than 1,000 residents are required to receive notifications, the incident must also be reported to all consumer reporting agencies with specific information. This would include the state attorney general and for medical, the Commissioner of Health too.
Notifications
Notifications to the consumer may require detailed information and sometimes provision of services. The notifications must be sent or delivered in a specific manner.
The notification may be delivered by mail, telephone, or electronically (consistent with US Code Section 7001 of Title 15). A substitute notice can be sent if the business demonstrates that the cost of providing the notice would exceed $50,000 or the persons to be notified exceeds 100,000, or they do not have sufficient contact information or consent. Substitute notice must consist of ALL of the following: email notice, conspicuous posting on their website, and notification to major statewide media.
Penalties
In almost all states, the state attorney general may bring action upon an entity that has not complied with their breach and/or consumer notification laws.
The state attorney general has enforcement and authority to bring an action to address violations and impose a civil penalty not to exceed $150,000 per breach of the security of the system or series of breaches of a similar nature that are discovered in a single investigation. Individuals also have the right to recover direct economic damages due to a violation.

CSR®
Privacy Made Simple℠

Applicable Laws
For more information, review your state statutes.
The statutes include, but are not limited to: Code of Virginia: • 18.2 Crimes and Offenses Generally Chapter 6 - Crimes Involving Fraud § 18.2-186.6. Breach of personal information notification • Title 32.1. Health Chapter 5 - Regulation of Medical Care Facilities and Services § 32.1-127.1:05. Breach of medical information notification. All entities should ensure there are no additional statutes applicable to them due to their type of business or activity. In addition, entities should ensure they have complied with federal laws or industry regulations that may also apply. For entities with out-of-country personal data, laws in those countries should also be reviewed for applicability.
Other Related Laws
In order to ensure protection of personal information BEFORE a breach happens, many states now have laws for data protection, data retention, and/or data disposal.
The statutes include, but are not limited to: Code of Virginia • Title 32.1. Health Chapter 5. Regulation of Medical Care Facilities and Services § 32.1-127.1:01. Record storage. § 32.1-127.1:03. Health records privacy • Title 2.2. Administration of Government Chapter 38. Government Data Collection and Dissemination Practices Act § 2.2-3808. Collection, disclosure, or display of social security number • Title 59.1. Trade and Commerce Chapter 35. Personal Information Privacy Act § 59.1-443.2. Restricted use of social security numbers § 59.1-443.3. Scanning information from driver's license or identification card; retention, sale, or dissemination of information.

Other Related Laws (cont'd)

- 18.2 Crimes and Offenses Generally
  Chapter 6 - Crimes Involving Fraud
  § 18.2-194. Unauthorized possession of two or more signed credit cards or credit card numbers.

All entities should ensure there are no additional statutes applicable to them due to their type of business or activity. In addition, entities should ensure they have complied with federal laws or industry regulations that may also apply. For entities with out-of-country personal data, laws in those countries should also be reviewed for applicability.