Publications
June 01, 2014
SECURITY BREACH NOTIFICATION CHART - Virginia

Va. Code § 18.2-186.6 (effective July 1, 2008),

§ 32.1-127.1:05 (effective January 1, 2011);

Amendment to **§ 18.2-186.6** (HB 2113) (effective July 1, 2017)

H.B. 2396 (signed into law March 18, 2019) (effective July 1, 2019)

Application. An individual, government entity, or any other legal entity, whether for profit or not for profit (collectively, Entity) that owns or licenses computerized data that includes PI.

- A separate provision covering health information applies only to government entities.

Security Breach Definition. Unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of PI maintained by an Entity as part of a database of PI regarding multiple individuals and that causes, or the Entity reasonably believes has caused, or will cause, identity theft or other fraud to any resident of VA.

- Good-faith acquisition of PI by an employee or agent of an Entity for the purposes of the Entity is not a breach of the security of the system, provided that the PI is not used for a purpose other than a lawful purpose of the individual or entity or subject to further unauthorized disclosure.

Notification Obligation. An Entity to which the statute applies shall disclose any breach of the security of the system to any affected resident of VA.

- An Entity shall disclose the breach of the security of the system if encrypted information is accessed and acquired in an unencrypted form, or if the security breach involves a person with access to the encryption key and the Entity reasonably believes that such a breach has caused or will cause identity theft or other fraud to any resident of VA.
- For health information, the Entity must notify both the subject of the medical information and any affected resident of VA, if those are not the same person.

Notification to Consumer Reporting Agencies. In the event an Entity provides notice to more than 1,000 persons at one time pursuant to the general security breach section, the Entity shall notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C. Section 1682(a)(p), of the timing, distribution, and content of the notice.

Attorney General/Agency Notification. The state AG must be notified whenever any VA residents are notified under the criteria above. In the event an Entity provides notice to more than 1,000 persons at one time pursuant to this section, the individual or entity shall notify, without unreasonable delay, the state Attorney General of the timing, distribution, and content of the notice. For health information, the Entity must also notify the Commissioner of Health.

Attorney General Notification for Breach of Employee Income Tax Data. Employers or payroll service providers that own or license computerized data relating to state income tax withheld must notify the Attorney General of unauthorized access and acquisition of unencrypted and unredacted computerized data containing a

taxpayer identification number in combination with the income tax withheld for that taxpayer that compromises the confidentiality of such data and that creates a reasonable belief that an unencrypted and unredacted version of such information was accessed and acquired by an unauthorized person, and causes, or the employer or payroll provider reasonably believes has caused or will cause, identity theft or other fraud. For employers, the notification obligation applies only to information regarding its employees (not customers or other non-employees).

Such employer or payroll service provider shall provide the Attorney General with the name and federal employer identification number of the employer without unreasonable delay after the discovery of the breach. The Attorney General shall then notify the Department of Taxation of the breach.

Third-Party Data Notification. An Entity that maintains computerized data that includes PI that the Entity does not own or license shall notify the owner or licensee of the information of any breach of the security of the system without unreasonable delay following discovery of the breach of the security of the system, if the PI was accessed and acquired by an unauthorized person or the Entity reasonably believes the PI was accessed and acquired by an unauthorized person.

Timing of Notification. Notice required by the statute shall be made without unreasonable delay. Notice may be reasonably delayed to allow the individual or Entity to determine scope of the breach of security and restore the reasonable integrity of the system.

Personal Information Definition. 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 VA, 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;
- 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 accounts;
- Passport number; or
- Military identification number.

The health information breach law applies to the first name or first initial and last name with any of the following elements:

- 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
- 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.

PI does not include information that is lawfully obtained from publicly available information, or from federal, state, or local government records lawfully made available to the general public.

Notice Required. Notice shall include a description of the following:

- The incident in general terms;
- The type of PI or medical information that was subject to the unauthorized access and acquisition;
- The general acts of the individual or entity to protect the PI from further unauthorized access;
- A telephone number that the person may call for further information and assistance, if one exists; and

- Advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports.

Notice means:

- Written notice to the last known postal address in the records of the individual or entity;
- Telephone notice; or
- Electronic notice.

Substitute Notice Available. If the Entity demonstrates that the cost of providing notice will exceed $50,000, the affected class of VA residents to be notified exceeds 100,000 residents, or the individual or the Entity does not have sufficient contact information or consent to provide written, electronic or telephonic notice. Substitute notice consists of all of the following:

- Email notice, if the individual or the Entity has email addresses for the members of the affected class of residents;
- Conspicuous posting of the notice on the Entity's website, if the Entity maintains one; and
- Notice to major statewide media.

Exception: Own Notification Policy. An Entity that maintains its own notification procedures as part of an information privacy or security policy for the treatment of PI that are consistent with the timing requirements of this section shall be deemed to be in compliance with the notification requirements of this section if it notifies residents of VA in accordance with its procedures in the event of a breach of the security of the system.

Exception: Compliance with Other Laws.

- **Gramm-Leach-Bliley Act.** An entity that is subject to Title V of the Gramm-Leach-Bliley Act and maintains procedures for notification of a breach of the security of the system in accordance with the provision of that Act and any rules, regulations, or guidelines promulgated thereto shall be deemed to be in compliance with this section.
- **Primary Regulator.** An entity that complies with the notification requirements or procedures pursuant to the rules, regulations, procedures, or guidelines established by the entity's primary or functional state or federal regulator shall be in compliance with this section.
- **HIPAA-Covered Entities.** The notification requirements for incidents involving medical information do not apply to (i) a "covered entity" or "business associate" subject to requirements for notification in the case of a breach of protected health information (42 U.S.C. § 17932 *et seq.*) or (ii) a person or entity who is a non–HIPAA-covered entity subject to the Health Breach Notification Rule promulgated by the Federal Trade Commission pursuant to 42 U.S.C. § 17937 *et seq.*

Penalties. The state Attorney General may impose a civil penalty not to exceed $150,000 per breach of the security of the system or a series of breaches of a similar nature that are discovered in a single investigation. (This provision does not apply to health information breaches.)

Other Key Provisions:

- **Delay for Law Enforcement.** Notice required by this section may be delayed if, after the Entity notifies a law enforcement agency, the law enforcement agency determines and advises the Entity that the notice will impede a criminal or civil investigation, or homeland or national security. Notice shall be made without unreasonable delay after the law enforcement agency determines that the notification will no longer impede the investigation or jeopardize national or homeland security.
- Attorney General Enforcement.