Security Breach Notification Laws in Virginia

By Jonathan M. Joseph and Noelle M. James

As more and more data is being stored electronically, businesses and organizations are at an increased risk of data security breaches. While the health care sector has been slow to utilize electronic data storage, security concerns for this method of data storage are now at the forefront for the industry due to federal efforts to spur use of electronic health records, and the increased use of electronic data by vendors to health care providers.

At the federal level, Congress has enacted data breach notification requirements through the Health Information Technology for Economic and Clinical Health Act (HITECH), which is part of the American Recovery and Reinvestment Act of 2009 (ARRA) and was signed into law in February 2009.

At the state level, 46 states, including Virginia, have enacted data breach notification laws. Unlike most states, Virginia has a statute that governs notification for breach of personal information, and a separate statute to govern notification for breach of medical information. While these two statutes contain similar requirements, there are a few important differences.

Who is Governed

The personal information statute (Virginia Code §18.2-186.6) is broad in its application and applies generally to all legal entities, public and private. The medical information statute (Virginia Code §32.1-127.1:05) only applies to public bodies and entities that are primarily supported by public funds.

Type of Information Accessed

The personal information statute applies when the information breached includes an individual's name in combination with any one of the following: (1) more than five digits of a Social Security number, (2) more than the last four digits of a driver's license number or state identification card number, or (3) more than the last four digits of a financial account number, credit card number or debit card number with any required security code that would permit access to an individual's account.

The medical information statute applies when the information breached includes an individual's name in combination with: (1) any information regarding an individual's medical or mental health history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or (2) more than four digits of an individual's health insurance policy number, subscriber identification number, or a unique identifier used by a health insurer; or (3) any information in an individual's application and claims history, including appeals records.

Neither statute is triggered if the compromised personal or medical information is redacted or encrypted and does not involve a person with access to the encryption key.

When Notification is Required

The personal information statute only requires notification to affected individuals if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person and there is a reasonable belief the data breach will cause identity theft or other fraud to any resident of Virginia. However, the medical information statute has a lower threshold for mandatory notification, which is triggered by the fact that the information was accessed by an unauthorized party—regardless of the likelihood the information will be misused.

Notification to Affected Individuals

Both statutes permit notification by mail to the last known address that the business or organization has for the affected individual.

There is no statutory requirement for due diligence in terms of locating affected individuals. As an alternative, the statutes permit notice by telephone or email. In certain circumstances, the statutes allow for alternate notification through major statewide media and the entity's website if the expense of other notification methods exceeds $50,000 and more than 100,000 Virginia residents are affected.

The required content for notification to affected individuals is fairly similar. Both statutes require that the communication:

- inform the individual of the circumstances around the data breach;
- disclose the type of information that was compromised;
- explain what the entity has done to protect against further security breaches; and
- provide a telephone number for further information and assistance.

The personal information statute also requires that the notification include advice directing individuals to be vigilant by monitoring their account statements and free credit reports.

Notification to State Agencies

In addition to providing notification to the affected individuals, the personal information statute requires that the Office of the Attorney General (OAG) be notified, and the medical information statute requires that both the OAG and the Commissioner of Health receive notice. While not statutorily required, guidance from the OAG requests that such notice include:

- a cover letter on the entity's official letterhead providing notice of the security breach;
- the approximate date of the security breach and how the breach was discovered;
- the cause of the security breach;
- the number of Virginia residents affected by the security breach;
- an explanation of steps taken to remedy the breach; and
- a sample of the notification sent, or to be sent, to affected individuals.

The personal information statute also includes a requirement that the major consumer credit reporting agencies be notified of the security breach when more than 1,000 residents are affected.

Timing of Notification

The statutes require that notice be provided to affected individuals and state agencies "without unreasonable delay." However, they provide for a delay in notification if law enforcement determines and notifies the organization that notification would impede an investigation or national security.

Exemptions

Both statutes provide an exemption for entities that comply with security breach notification requirements and procedures pursuant to regulations and procedures established by the entity's primary or functional state or federal regulator. The medical information statute also provides an exclusion for a "covered entity" or "business associate" that is already subject to notification requirements for breach of protected health information under HIPAA.

It should also be noted that the applicability of the federal HITECH Act is limited to entities that are HIPAA “covered entities” and/or HIPAA “business associates” or specified vendors of personal health records. In many instances, entities in the health care industry will not fall within the definitions of entities subject to federal breach notification laws. Therefore, when analyzing a breach situation it is important to closely exam the entity involved and the applicability of federal and state law.

Other Considerations

Many of the state security breach notification laws, including Virginia's, are triggered by a data security breach affecting residents of the state regardless of where the business or data was located. Therefore, in the event of a data breach in Virginia, it may be necessary to consider other state laws beyond where the business primarily operates.

Given the myriad of state requirements, advanced planning is extremely helpful and is recommended. Analysis of an organization’s stored electronic information, such as a breakdown of location by state and the type of data on the system, is extremely helpful in preparing to address the consequences of a security breach. Early efforts to locate advisors on handling data breach situations will save needed time that can be devoted to addressing the security breach and the notification requirements. Maintaining insurance policy protection for losses and damages that can arise from a data security breach also should be considered. In addition, it is important to regularly review the applicable laws and regulations for changes.

Hopefully, the information in this article will never be needed. But the realities are that data security breaches may occur even in the best run organizations—and preparation is the best defense.

For additional information, please contact:
Jonathan M. Joseph, Esq.
Christian & Barton, LLP
909 East Main Street, Suite 1200
Richmond, Virginia 23219
jjoseph@cblaw.com | 804.697.4125