

## Articles - Other

### **Once More Into the Breach** *Business NH Magazine*

We live in an age of technology, where we swipe increasingly smaller plastic cards containing our personal and financial information for gas, groceries and every convenience in between, and we provide personal information to all kinds of businesses. This age, however, has also brought escalating reports of security breaches compromising that data.

To protect consumers, the state of New Hampshire imposed new obligations on anyone doing business in the state that maintains personal information in electronic form. The Notice of Security Breach law took effect January 1, 2007. It is time to update policies and procedures for security breaches and unauthorized acquisition of personal information to assure compliance with the latest requirements.

The Notice of Security Breach obligations apply to any individual, corporation, trust, partnership, limited liability company, or other type of entity. They also apply to any agency, authority, board, court, department, division, commission, institution, bureau or other state governmental entity, and any political subdivision of the state. Even for those entities already subject to the Health Insurance Portability and Accountability Act ("HIPAA"), this law is more stringent than HIPAA and imposes additional requirements.

The new law defines personal information as a person's first name or initial and last name **plus** any of the following, when either the name or the following is not encrypted: a social security number; a driver's license number or other government identification number (e.g. Medicare, Medicaid or professional license numbers); or an account, credit card or debit card number, in combination with any security or access code or password to permit access to a person's financial account.

Under this law, personal information does *not* include information that is lawfully made available to the general public from federal, state or local government records, nor does it include personal information when both the name and the data elements are encrypted. However, simply requiring a key, security code, access code or password does not qualify the data as encrypted under this statute.

This law imposes new notification requirements if there is a security breach. A "security breach" means any unauthorized acquisition of personal information maintained in an electronic format that compromises the security or confidentiality of that information.

Businesses facing such a breach must promptly determine whether it is likely that personal information has been or will be misused. If a misuse of the data has occurred or is reasonably likely to occur, or if you cannot make that determination, you must notify all affected individuals as soon as possible.

In addition, businesses must notify the NH Attorney General's Office and, in most cases, industry regulators. Notice to the applicable regulator or Attorney General's Office must include the anticipated date you will give notice to affected individuals and the approximate number of individuals in New Hampshire who will be notified.



**SHEEHAN  
PHINNEY  
BASS +  
GREEN PA**  
*the business law firm*

Further, if there are more than 1,000 affected persons, you must *also* notify all of the national consumer reporting agencies, giving them the anticipated date of the notification to consumers, the approximate number of persons affected and the content of the notice.

Delay in notification is permitted if a law enforcement, national or homeland security agency determines that giving the notification will impede a criminal investigation or jeopardize national or homeland security.

The new law permits you to give notice in several ways - in writing, via electronic notice if this is your usual primary means of communication with the affected persons, by telephone if you keep a log of each notification, or by what is called "substitute notice." There are exceptions for cases where the cost of making the notice would exceed \$5,000, where there are more than 1,000 people to notify, or where you do not have sufficient contact information to reach the affected people. In these cases, you may notify those affected by e-mail, if you have the addresses; through a posting to your Web site, if you maintain one; or by notice via a major statewide media outlet.

The notice itself must include a description of the security breach incident in general terms, the approximate date of the breach, the type of personal information that was obtained as a result of the security breach, and your telephone contact information.

The New Hampshire Attorney General's Office is responsible for enforcement of the new law while the burden of demonstrating compliance rests on the business. An updated security breach policy is a smart idea for any business in New Hampshire that collects and stores electronically personal data from its customers, clients or patients.