Pillsbury Winthrop Shaw Pittman LLP

Health Care
Privacy & Data Protection
January 14, 2008

Client Alert

# California's Data Breach Notification Law Now Covers Medical and Health Insurance Information

by Edgar D. Bueno, John L. Nicholson, and Melissa M. Starry

**Going well beyond the requirements of HIPAA and most state health privacy laws, California has amended its existing Database Security Breach Notification Act to require any organization that reasonably believes a breach of a California resident's medical or health insurance information has occurred, to notify that resident. Any entity that owns, licenses, or possesses unencrypted data containing the personal health information of any California resident should be aware of this new requirement and its potentially broad application, since those subject to this law could be anywhere in the United States.**

Theft of laptops, loss of data, improper access and other security breaches involving unencrypted personal health information could trigger the law's burdensome notification requirements. Accordingly, individuals and business entities should carefully evaluate the information they collect and store, how they store it, and develop a plan to respond to any breach of the security of patient health information and records.

## Amendment Expands Existing Notification Requirements

The California Database Security Breach Notification Act ("SB 1386")[1] requires notification to California residents if certain types of unencrypted "personal information" are determined or reasonably believed to have been improperly accessed by unauthorized individuals. The amendment to SB 1386, which went into effect on January 1, 2008, expands the definition of "personal information" to include "medical information" and "health insurance information."

Specifically, "medical information" is defined as "any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional."

[1] CAL. CIV. CODE §§ 1798.29, 1798.82.

"Health Insurance Information" is defined as "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."

## Scope of the Notification Requirement

Any business with employees in California or any business in the healthcare or health insurance industry that owns, licenses or maintains electronic data that contains medical or health insurance information about California residents may be affected by the law's notification requirements.

The law requires specific remedial steps be taken and documented as part of the notification process. Other measures beyond individual notification may also be required depending on the circumstances of the breach. Currently, under federal privacy laws, health care providers and other covered entities have only limited accounting and disclosure obligations with respect to data breaches.

The California law's most significant impact may be felt by those organizations or employers who merely maintain or "house" medical or health insurance information concerning their own employees or other individuals as part of their business. For example, if a data breach occurs at a small health information technology company, the law would require such company to notify all of those individuals whose unencrypted medical information may have been acquired by any unauthorized person.

Under the law, notice to affected individuals may be provided by either written or electronic means.[2] If the cost of either method exceeds $250,000 or the number of individuals to be notified exceeds 500,000, then an organization may use substitute notice. The substitute notice provisions require an organization to: (1) notify the California resident by e-mail, (2) make a conspicuous posting of the notice on the organization's web site, and (3) provide notification to major California media. Notably, however, the law also permits notification in compliance with an organization's internal notification policies provided that the timing of such notification is consistent with California law. Notification may be temporarily delayed to determine the scope of the breach and restore system integrity, or if immediate notification would impede a criminal investigation.

A company's brand or reputation can be materially damaged if it is viewed as remiss or derelict when it comes to protecting personal health information. For that reason alone, organizations should take steps to minimize the likelihood of any data breach that would require notice under the new law. In addition, the failure to provide the requisite notice may also lead to civil liability and possible injunction. An individual injured by an organization's failure to provide notice may also initiate a civil action.

## Recommendations

Any organization that owns, licenses or maintains electronic data that contains medical or health insurance information about California residents should:

- Review their policies and procedures and consider whether that medical and health insurance information is necessary for the organization's business;
- Identify key systems containing such medical or health insurance information, and activate and enhance logging capabilities on such systems and/or deploy network monitoring technologies;

[2] Provided such notice is consistent with provisions regarding electronic notice and signature set forth in 15 U.S.C. § 7001.

- Evaluate how medical and health insurance information is stored and used and consider the costs and benefits of encryption of such information, both in transit and at rest;
- Review contracts with other parties involving the transfer of medical or health insurance information (including those related to offsite data storage) to confirm that such contracts contain information-security provisions, including mandatory notification, rights to investigate, and right to participate in or control reporting decisions involving customer data; and
- Draft an incident response plan that:
  - Requires notification of counsel's office or incident response team when breach of key systems has been detected;
  - Specifies a mandatory period for investigation and remediation before decisionmaking with regard to third-party notifications; and
  - Provides a notification plan (at least for California residents) on terms more flexible than the substitute notice provisions of SB 1386.

The original version of SB 1386 was responsible for the earliest reports of data breaches becoming public knowledge. Following its implementation and the resulting disclosures, many states adopted similar laws. The new amendment to SB 1386 makes it more likely that news of a data breach involving medical or health insurance information will become public knowledge, and it is likely that other states will follow California's lead, again. Organizations that own, license or maintain electronic data that contain medical or health insurance information, regardless of whether such information pertains to California residents, should prepare for the possibility that such a law will be implemented in their states as well.

For assistance with regard to data security policies and procedures, or for further information, contact:

**David C. Main** (bio)
Northern Virginia
+1.703.770.7518
david.main@pillsburylaw.com

**Edgar D. Bueno** (bio)
Northern Virginia
+1.703.770.7709
edgar.bueno@pillsburylaw.com

**Deborah Thoren-Peden** (bio)
Los Angeles
+1.213.488.7320
deborah.thorenpeden@pillsburylaw.com

**Catherine D. Meyer** (bio)
Los Angeles
+1.213.488.7362
catherine.meyer@pillsburylaw.com

**Jeffrey S. Ross** (bio)
San Francisco
+1.415.983.1730
jeff.ross@pillsburylaw.com

**Melissa M. Starry** (bio)
Northern Virginia
+1.703.770.7746
melissa.starry@pillsburylaw.com

**John L. Nicholson** (bio)
Washington, DC
+1.202.663.8269
john.nicholson@pillsburylaw.com