PUBLICATION

California (and Texas) Increase Privacy Requirements [Ober|Kaler]

2012: Issue 1 - Focus on HIPAA/Privacy

In 2012, new statutes in California and Texas will require that providers make state-specific changes to their existing privacy compliance procedures. The changes made in California are detailed below. Texas's new law is addressed in "Texas (and California) Increase Privacy Requirements."

California's Senate Bill 24 (SB 24), which took effect on January 1, 2012, makes substantial modifications to sections 1798.29 and 1798.82 of the Civil Code, two of the state's several data breach notification laws. Section 1798.82 applies to any person or business that conducts business in California, and in effect appears to serve as the state's "floor" provision, applying certain data breach reporting responsibilities to essentially every entity doing business in the state. In addition, under existing California law, certain *licensed* health care providers are subject to separate, additional breach notification law – Health & Safety Code § 1280.15, for example, which imposes additional specific obligations (including a five-day disclosure deadline) on the specifically identified entity types. SB 24 makes no changes to these existing requirements.

SB 24 was drafted, according to one of the bill's sponsors, to repair what was seen as a deficiency in existing state law breach notification laws. Although existing law required that notifications be sent in certain circumstances, it did not specify the *content* of those notices, nor did it require that notice be provided to any state officials in the event of an especially large breach. SB 24 addresses these concerns.

SB 24 applies to "any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information." *Personal information* is defined by the bill to include:

An individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

1. Social security number.
2. Driver's license number or California Identification Card number.
3. Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.
4. Medical information.
5. Health insurance information.

SB 24 specifically excludes any information that is publicly available through government records. SB 24 defines *medical information* to include "any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional" and *health insurance information* to include "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." In practical application, SB 24 will extend to cover most health care providers (licensed or not) whether or not they are considered a covered entity or business associate under HIPAA.

SB 24 requires that entities subject to the bill disclose any "breach in the security of the data" to any "residents of California" whose data security may have been compromised "in the most expedient time possible and

without unreasonable delay." The bill goes on to provide, however, that such notice should be timed to be "consistent with the needs of law enforcement…or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system."

A *breach of the security of the system* is defined to include any unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained…" A breach, however, is defined to specifically exclude a "good faith acquisition of personal information by an employee or agent of the business for the purposes of the person or business…provided that the personal information is not used or subject to further unauthorized disclosure."

Entities, including providers, subject to SB 24 may provide notice through several means:

- Written notice, sent to a physical address, or
- Electronic notice, so long as the notice is provided consistent with the provisions of electronic records and signatures set forth in section 7001 of Title 15 of the United States Code.

Where the person or business can demonstrate that the cost of providing notice through written or electronic means would exceed $250,000, or that the affected class of persons exceeds 500,000, or that the person or business required to provide the notice does not have sufficient contact information to provide the required notice, "substitute notice" may be provided. *Substitute notice* requires *all of*:

- Email, where the person or business has an email address for the subject persons;
- Conspicuous posting of the notice on the business's web site; and
- Notification to "major statewide media and the Office or Privacy Protection within the State and Consumer Services Agency."

In addition, SB 24 provides that a person or business that "maintains its own notification procedures as part of an information security policy" may provide notice in the method specified in that policy so long as the notice is provided in accordance with the bill's timing requirements and in accordance with "its policies in the event of a breach of the security of the system."

Security breach notifications must be written in "plain language" and include, at the minimum:

- The name and contact information of the reporting person or business subject to this section;
- A list of the types of personal information that were or are reasonably believed to have been the subject of a breach;
- If the information is possible to determine at the time the notice is provided, then any of the following:
  - the date of the breach,
  - the estimated date of the breach, or
  - the date range within which the breach occurred;
- The date of the notice;
- Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided;
- A general description of the breach incident, if that information is possible to determine at the time the notice is provided; and
- The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or a driver's license or California identification card number.
- In addition, at the discretion of the person or business providing the notice, the notice may include the following:

- Information about what the person or business has done to protect individuals whose information has been breached, and
- Advice on steps that the person whose information has been breached may take to protect himself or herself.

Finally, it is important to note that these provisions apply only where an entity is *not* a “covered entity” as defined under HIPAA. Covered entities, which are already subject to the Interim Final Breach Reporting Rule, will be deemed to have complied with the state's notice requirements when they comply with the federal requirements.

Regardless of an entity's status under federal law, however, in the event of a single breach involving more than 500 California residents SB 24 requires more than notice to the affected individuals (even when such notice is provided according to federal requirements). The entity providing the notice must also electronically submit a single copy of the notice being provided (excluding any personal information) to the California Attorney General.

Ober|Kaler's Comments

California's requirements are, for the most part, consistent with those required under the HITECH Act's Interim Final Breach Reporting rule and should not pose substantial compliance burdens for most providers. California's laws, however, have a substantially broader reach than federal rules and apply to many businesses and data types that are generally not covered by HIPAA. Entities doing business in California should be careful to review *all* of the state's breach reporting rules and ensure that their policies and procedures are consistent with state requirements. A failure to do so can have significant consequences.