

Your Obligations Under the Data Breach Notification Statutes

By: Susan E. Gindin¹

There have been various federal and state initiatives to stem the serious problem of identity theft. Among them are the data breach notification requirements enacted because data breaches involving sensitive personal information may result in identity theft and financial crimes. The data breach notification statutes are intended to provide individuals with timely warning that their personal information may have fallen into the hands of an unauthorized person, giving them the opportunity to take action to protect themselves against identity theft or to minimize the effect of identity theft that has taken place.

Nearly every organization in the U.S. which handles personal information of individuals is subject to a data breach notification requirement. The Department of Health & Human Services ("HHS") and Federal Trade Commission ("FTC") have just issued specific health data breach notification requirements ("Health Data Breach Notification Requirements") pursuant to the American Recovery and Reinvestment Act of 2009 (the "Recovery Act") and which govern HIPAA covered entities, business associates, and vendors of personal health records (PHR) and related entities and service providers. There are also security breach notice guidelines issued pursuant to the Gramm Leach Bliley Act and which apply to financial institutions ("GLB Guidelines").

Also, there are data breach notification statutes in 45 states and the District of Columbia. Most statutes are modeled on the California statute (SB 1386) which took effect in 2003. As a result, these statutes resemble each other but with subtle differences in definitions, deadlines for notifications, and details. Data breaches often affect individuals in more than one state, and therefore organizations which experience breaches must comply with the varying statutes in effect in every state in which their customers reside.

State Statutes Generally

The state laws generally require entities to notify consumers when there has been a breach that exposes their personally identifiable information. Colorado's statute, which is fairly typical, applies to any individual or commercial entity which owns, licenses, or maintains personal information about a resident of Colorado. The Health Data Notification

¹ Copyright ©2009 Susan E. Gindin. Susan Gindin is Of Counsel to Isaacson Rosenbaum P.C. where she specializes in the areas of data privacy and security, advertising, new media, information technology and intellectual property law. Susan has been practicing in the area of data privacy and security law for more than thirteen years.

Your Obligations Under the Data Breach Notification Statutes

Page 2

Requirements apply to any entity subject to the Recovery Act that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured protected health information.

Definition of "Personal Information"

Most state statutes, including Colorado's, define "personal information" as any data that associate an individual's name with either his/her Social Security number, driver's license number or a financial account number in combination with any required security code or password that would permit access to the resident's financial account. Some statutes include biometric data including fingerprints and DNA profiles. California and Arkansas include health information.

Type of Data and Safe Harbors for Secure Handling

Most state notification laws (like Colorado's) apply to computerized data, although a few states' notification requirements (and the Health Data Notification Requirements) apply to hard copy data as well. Most statutes (including Colorado's as well as the Health Data Notification Requirements) have a safe harbor exempting notification if the data is effectively encrypted. Also, most states, like Colorado, do not require notification if it is determined, through investigation, there is no reasonable likelihood of harm to the individuals. Others require entities to make notifications upon discovery or knowledge of the breach regardless of its potential impact on them.

Notice Deadlines

Time frames for notification vary. Most states, including Colorado, require that an entity notify affected individuals "in the most expedient time possible and without unreasonable delay" but some states have 45 day and shorter notification time frames. The Health Data Notification Requirements are that the notice shall be made without unreasonable delay and in no case later than 60 calendar days after the discovery, and the FTC proposed regulations for vendors of personal health records require such entities to notify the FTC in the event a breach affects 500 or more individuals in five business days.

Like many data breach notification statutes, Colorado's statute also allows the individual or entity to delay notification if a law enforcement agency determines that the notification would impede a criminal investigation. Colorado also allows delay to restore the integrity of the computer system.

Notice Requirements

Like many states, Colorado law requires notice by mail, phone, or email if that is the traditional means of contact. Most state laws allow a substitute form of notice in certain circumstances. For example, Colorado's law provides that if the individual or the entity required to provide notice demonstrates that the cost of providing notice will exceed \$250,000, the affected class of persons to be notified exceeds 250,000 Colorado residents, or the individual or entity does not have sufficient contact information to provide notice, Colorado allows substitute notice in the form of email notice if the individual or entity has email addresses; conspicuous posting of the notice on the individual's or entity's web site; and notification to major statewide media.

Your Obligations Under the Data Breach Notification Statutes

Page 3

Some states also require notification to credit bureaus and regulators. For example, if more than one thousand residents are affected, Colorado requires the person or entity to notify the consumer reporting agencies of the notification to the residents and the approximate number of residents who are to be notified.

Some states also exempt organizations from certain notification requirements if the organization is already complying with a federal law or guidelines. For example, Colorado exempts organizations from notifying the credit reporting agencies if they are subject to the GLB Guidelines.

The Health Data Breach Notification Requirements are very exacting. For more detail regarding the Health Data Breach Notification Requirements, see Susan E. Gindin's *Understanding The Stimulus Package's Changes To HIPAA's Privacy Provisions* at <http://www.ir-law.com/5FBFD1/assets/files/lawarticles/UNDERSTANDING%20THE%20STIMULUS%20PACKAGE1.pdf>

Information Security Requirements

In addition, an increasing number of states are enacting specific requirements regarding how personal information should be handled. The most stringent to date are the Massachusetts regulations issued pursuant to the Massachusetts security breach law. These regulations set minimum standards for the protection of personal information and apply to personal information located anywhere, about Massachusetts residents. These regulations, which take effect January 1, 2010, require that organizations encrypt personal information that is stored on laptops or flash drives, or that is transmitted over the Internet or wireless.

How Should Organizations Prepare for Data Breaches

If your organization handles personal information in any format, there are important steps you should take:

A necessary step is to know your state's data breach notification laws, and also the state laws where your customers live. In the event you experience a security breach, you need to know these laws in order to investigate whether the security breach rises to a reportable breach, and to comply with the various laws when making any necessary notifications.

However, the best way to avoid liability from state breach laws is to prevent a data breach from occurring in the first place. In addition to avoiding the data breach notification requirements, companies can avoid the extraordinary costs of dealing with a data breach. According to a recent study by the Ponemon Institute (http://www.cenzic.com/downloads/Ponemon_Study_2008.pdf), it costs \$6.6 million on average when a company suffers a data breach, and more than \$200 per compromised record. According to the Ponemon Study, most of this cost is lost business.

In order to avoid a data breach, your organization needs a comprehensive information security plan. Although guidance regarding development of a comprehensive information security plan is beyond the scope of this article, a key component is ensuring that all data

Your Obligations Under the Data Breach Notification Statutes

Page 4

(whether in hard copy, hard drives, or storage media, including laptops and portable devices) is protected.

The HHS Guidance issued in April provides specific instruction that what makes electronic data unusable, unreadable or indecipherable are only two methods: encryption (provided the encryption key has not been compromised) and effective destruction. These methods are key for any organization handling health care data because they provide a safe harbor from the notification requirements but also will likely become the de facto standard of care with regard to handling of personal data of all kinds.

HHS has recently asked for comments regarding whether there are additional means for securing data, but until HHS acknowledges such additional means, effective encryption and destruction are the only accepted methods for securing data for the purposes of qualifying for a safe harbor from the notification requirements. For more information about the HHS Guidance and your opportunity to comment, see Susan Gindin's accompanying article, *HHS and FTC Issue Guidance Regarding the Health Data Breach Notification Provisions and Invite Comment*.

As noted, encryption of electronic data also offers a safe harbor from most state data breach notification requirements. Moreover, in addition to the fact that if the personal data is effectively encrypted, you have a safe harbor under most data breach notification laws, you are also likely to avoid a data breach in the first place. Furthermore, in effectively safeguarding the personal information of your customers, you will better protect your customers, as well as your reputation.

If you have any questions about the data breach notification laws, or any other information privacy or security issues, please contact Susan Gindin at 303-256-7046 or sgindin@ir-law.com.