Keeping Up With The Breach Notice Laws: 4 Common Misconceptions

Rebecca Herold, CIPP, CISSP, CISA, CISM, FLMI
Final Draft for June 2008 CSI Alert

Over the past few months there have been some changes in U.S. breach notice laws; as of May 9, 2008, there were at least 43. ***(3/28/09 NOTE: this number is now 47)*** You can see a listing of them at http://www.privacyguidance.com/elegal_regulations.html. During the CSI SX conference at the end of April, and at other seminars and conferences this year, I've chatted with many information security and privacy practitioners, and there are some widespread misconceptions about the breach notice laws that I want to address here.

Misconception #1: The definitions of personally identifiable information (PII) are the same for all the laws

It is important to know that the definitions of PII within each of the U.S. breach notice laws are not all the same!

You need to include the widest definition of PII within your incident response plans. Within the U.S. and specific to the privacy breach laws, the first definition, as put forth by California SB 1386 in 2004, was very limited in scope:

> *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.*

However, when California's new law, AB 1298, took effect January 1, 2008, becoming the second state after Arkansas to include medical and health information in the definition of "personal information," organizations nationwide took note about the broader definition of PII. This impacted not only the triggers within security incident and breach response plans, but also the impacts, to individuals as well as organizations, for breaches. The risks involved with medical PII breaches are different than financial PII breaches.

Medical PII can include a very wide scope of information, such as medical history, diagnosis, policy number, subscriber number, an application, claims history, and appeals history, according to the laws.

The change in the definition of PII in these breach notice laws shifted the focus from preventing identity theft and financial crimes to preventing a very wide range of fraud, crime, and even physical harm that could occur through the compromise of medical information.

Don't forget about the definitions of PII within data protection laws outside of the U.S. While am not aware of any current breach response laws outside the U.S., there are at least 100 data protection laws throughout the world that include a definition of PII. Your organization needs to protect that PII according to the associated requirements. However, it is important to be aware that Australia is considering the passage of a breach law and the European Parliament is drafting a breach notice law covering data transfers within not only the European Union countries, but also with the U.S.

Misconception #2: All breach laws require notification

Many information security and privacy practitioners believe that the breach notice laws always require notification to the individuals for whom the involved information applies. However, there are basically two kinds of breach notice laws currently in effect.

Always notify

Some laws require notification regardless of whether or not the PII involved is encrypted, or other specifics related to the breach situation. Notification may be required to the impacted individuals and/or to the state Attorneys General offices. These are typically referenced as "strict liability" laws.

The following are just a few examples of states that require notification when it has been determined a security breach of basically any type has occurred.

- Hawaii Rev. Stat. § 487N-2 requires, *"(a) Any business that owns or licenses personal information of residents of Hawaii, any business that conducts business in Hawaii that owns or licenses personal information in any form (whether computerized, paper, or otherwise), or any government agency that collects personal information for specific government purposes shall provide notice to the affected person that there has been a security breach following discovery or notification of the breach*."
- New Hampshire 359-C:20 states, *"Any person doing business in this state who owns or licenses computerized data that includes personal information shall, when it becomes aware of a security breach, promptly determine the likelihood that the information has been or will be misused. If the determination is that misuse of the information has occurred or is reasonably likely to occur, or if a determination cannot be made, the person shall notify the affected individuals as soon as possible as required under this subdivision."*

Notify based upon threshold analysis

Those that require notification based upon likelihood that the PII was accessed, misused, actually resulted in harm, and so on. These laws require a type of threshold analysis. Some of these states include:

- Idaho Code §§ 28-51-104 to 28-51-107 states, *"(1) An agency, individual or a commercial entity that conducts business in Idaho and that owns or licenses computerized data that includes personal information about a resident of Idaho shall, when it becomes aware of a breach of the security of the system, conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused. If the investigation determines that the*

misuse of information about an Idaho resident has occurred or is reasonably likely to occur, the agency, individual or the commercial entity shall give notice as soon as possible to the affected Idaho resident."

- Indiana Code IC 24-4.9-2-3 states, "…*after discovering or being notified of a breach of the security of a system, the data base owner shall disclose the breach to an Indiana resident whose: (1) unencrypted personal information was or may have been acquired by an unauthorized person; or (2) encrypted personal information was or may have been acquired by an unauthorized person with access to the encryption key; if the data base owner knows, should know, or should have known that the unauthorized acquisition constituting the breach has resulted in or could result in identity deception (as defined in IC 35-43-5-3.5), identity theft, or fraud affecting the Indiana resident.*"
- Louisiana La. Rev. Stat. § 51:3071 states, "*G. Notification under this title is not required if after a reasonable investigation the person or business determines that there is no reasonable likelihood of harm to customers."*

Whatever you do, be consistent!

Organizations that have tried to provide notifications only to those states whose laws always require notification in situations where actual harm resulting from the breach could not be confirmed have found themselves in hot water with the other states where they have customers, along with the Attorneys General in those states. By providing different types of notification to your customers you are risking that the customers you do not notify will interpret the decision as your organization being less caring about customers located in certain states.

There seems to be a trend in the laws to require notification based upon a harm likelihood analysis. Until that time, you need to discuss with your legal counsel the impact and need to always notify if you have customers in even just one state with such strict liability laws.

Misconception #3: All breach laws have an encryption "safe harbor"

Many of the breach notice laws only require notification if the PII is in electronic form and is not encrypted; in other words, having encrypted PII is a safe harbor for organization to keep them from needing to send notification. However, not all of the breach notice laws have this safe harbor. As the Indiana law previously listed shows, notification will still be necessary for encrypted data if the person accessing the information may have had access to the encryption key. The previously referenced New Hampshire law excerpt also demonstrates that encryption is not always mentioned with the laws.

As a couple of other examples:

- Massachusetts H.B. 4144, Chapter 93H states, *"'Breach of security', the unauthorized acquisition or unauthorized use of unencrypted data or, encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information, maintained by a person or agency that creates a substantial risk of identity theft or fraud against a resident of the commonwealth.*"

- Nevada Chapter 603A Rev. Stat. 603A.010 states, *"'Breach of the security of the system data' means unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of personal information maintained by the data collector."*

Be sure that your information security incident and breach response plans include actions to do whether or not the PII is encrypted. You will need to have a strong response team leader who can speak knowledgeably about this with your legal counsel whenever this situation occurs.

Misconception #4: All breach notice laws apply only to electronic PII

Many folks I've spoken with have expressed the belief that the breach notice laws only apply to PII in electronic form. However, many of the state laws apply to PII in any form.

As just a few examples:

- California's Civil Code Section 1798.80-1798.84 states that, "*'Records' means any material, regardless of the physical form, on which information is recorded or preserved by any means, including in written or spoken words, graphically depicted, printed, or electromagnetically transmitted.*"
- Hawaii's Rev. Stat. § 487N-2 states that, "*Any business that owns or licenses personal information of residents of Hawaii, any business that conducts business in Hawaii that owns or licenses personal information in any form (whether computerized, paper, or otherwise), or any government agency that collects personal information for specific government purposes shall provide notice to the affected person that there has been a security breach following discovery or notification of the breach."*
- Indiana's Code IC 24-4.9-2-2 states that, "*Sec. 2. (a) 'Breach of the security of a system' means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a person. The term includes the unauthorized acquisition of computerized data that have been transferred to another medium, including paper, microfilm, or a similar medium, even if the transferred data are no longer in a computerized format.*"

Growing numbers of privacy breaches are occurring as a result of improper printed papers disposal and stolen paper documents. Organizations need to ensure they have procedures implemented to know when PII in any form is inappropriately accessed. They must also ensure their information security incident and privacy breach notice plans include consideration of PII in all forms.

Rebecca Herold, CIPP, CISSP, CISM, CISA, FLMI, "The Privacy Professor"® is an information security, privacy and compliance consultant, writer and Norwich University MSIA adjunct professor. She produces the quarterly employee awareness tool, "Protecting Information" (http://www.privacyguidance.com/piqa_newsletter.html), the Security Search training event (http://www.privacyguidance.com/security_search.html) and blogs daily at http://www.realtime-itompliance.com. She can be reached at rebeccaherold@rebeccaherold.com or http://www.privacyguidance.com.