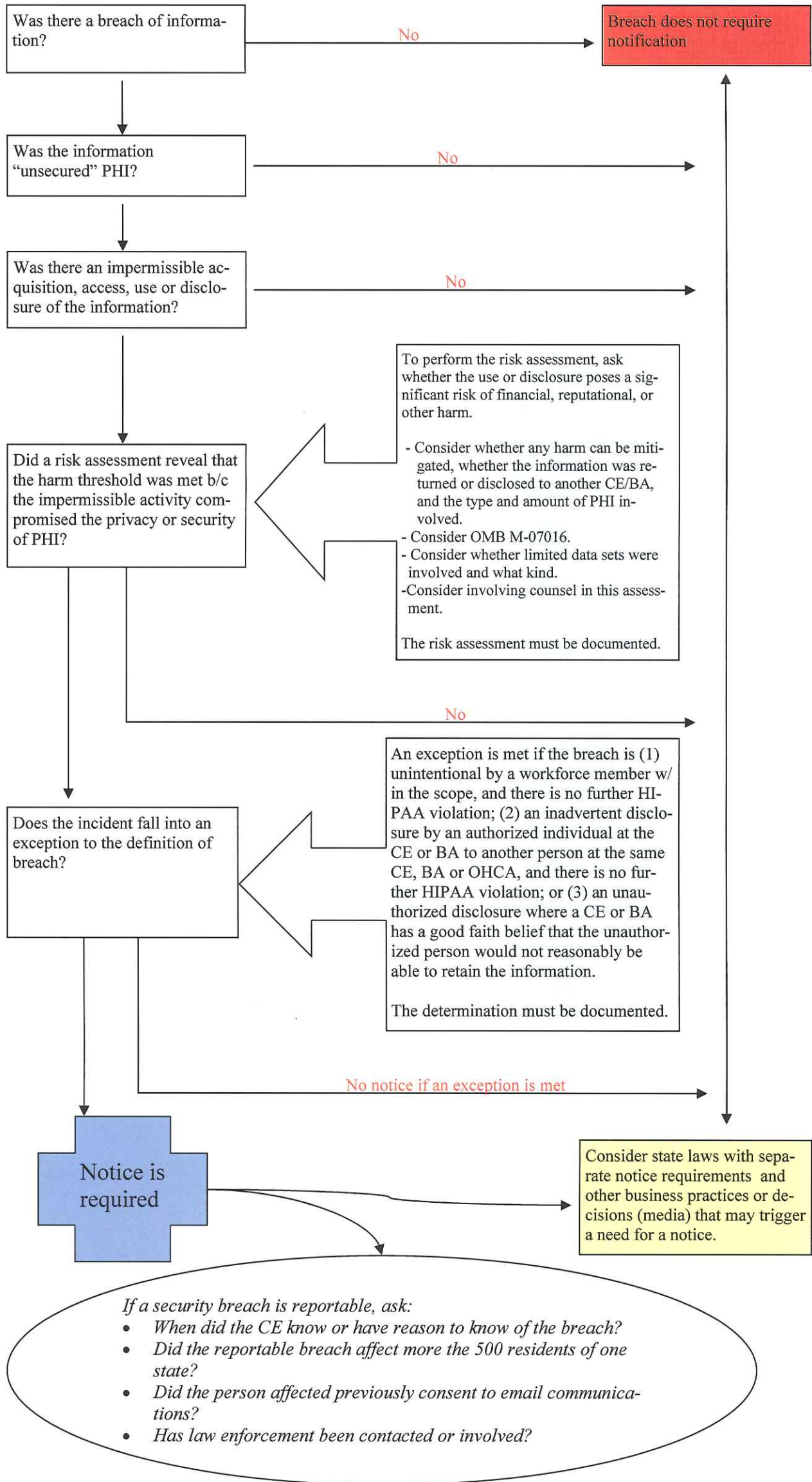


When a “Breach” Triggers Notification Obligations under the Health Information Technology for Economic and Clinical Health Act (HITECH) (45 CFR Part 164, Subpart D)

By Jackie Crain, Trenam Kemker Health Law Team





By: Jacqueline
M. Crain
E-Mail: jcrain@trenam.com

Identity theft is a serious threat. Data breaches leading to potential identity theft problems

have affected millions of consumers and a long list of organizations, including Countrywide Mortgage, TJ Maxx, ChoicePoint, the National Institutes of Health and the Department of Veterans Affairs. The Federal Trade Commission estimates that 9 million Americans have their identities stolen each year. Because millions of consumers have been affected by the unauthorized disclosure of personal and financial data by government agencies, private companies, educational institutions and other businesses, at least forty-four states have enacted laws requiring notification to consumers of security breaches.

In general, security breach notification laws are intended to provide notice to consumers when their personal information has been lost, stolen or inappropriately disclosed so that each consumer can protect against theft by closing accounts, notifying creditors, freezing credit reports, purchasing credit monitoring insurance, disputing unauthorized transactions and otherwise mitigating risks of the inappropriate or unauthorized release of sensitive data. Although the focus of these laws is on the protection of the consumer, the end result is that businesses need to be aware of the requirements, have a team prepared to investigate any breaches, and be ready to issue the appropriate notices.

In Florida, any person or business that conducts business in the state and “maintains computerized data in a system that includes personal information” is required to provide certain written notices if there is a breach of unencrypted data to an unauthorized person (or if there is reason to believe a breach of such data has occurred). Florida Statute 817.5681 sets forth the detailed requirements, which require notification “without unreasonable delay.” With some exceptions, most notices must be provided within 45 days. There are significant fines for failing to

provide the notices (\$1,000 per day for 30 days and then higher fines not to exceed \$500,000).

Florida’s security-breach notification law applies broadly to varying types of personal information. Unlike other state and federal laws that apply to certain specific types of data (personnel records, school records, medical records, benefits/claims records, financial/credit records), this statute reaches a variety of industries as it applies to “personal information”, which includes an individual’s first name, first initial and last name, or any middle name and last name, in combination with any one or more of the following data elements when the data elements are not encrypted:

- (a) Social security number.
- (b) Driver’s license number or Florida Identification Card number.
- (c) Account number, credit card number, 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.

Timing is a critical component of compliance with Florida Statute 817.5681. It is prudent for businesses to implement a policy (or a written process/guideline) to outline compliance with this statute or, at a minimum, the process that should be followed in response to a potential or actual computerized data breach. This process may be part of an organization’s security incident response plan, and should outline how the organization will collaborate with any vendor that maintains the pertinent information on its behalf. The policy should also assist the organization in determining whether the breach is likely to cause harm to individuals whose personal information has been acquired. Because business entities that maintain computerized data on behalf of other entities must provide certain notices to their clients or risk monetary fines similar to those mentioned above, many vendors (such as information technology vendors, collection agencies, and others) need a process for promptly investigating an incident, communicating with clients, and collaboratively working to alleviate any harmful effect on those individuals whose personal information may be involved.

In addition to policies, guidelines, incident team charters and other operational considerations, Florida businesses that maintain unencrypted computerized data should consider contractual provisions related to collaboration among vendors, notification language that permits longer time periods than consistent with the statute, the costs of notices to affected consumers, and indemnification for certain actions or inactions resulting in a breach of computerized data. After a laptop is stolen, wireless information systems are breached or there is employee misconduct, the deadline for notices will not leave time for the business to begin to organize the appropriate team and outline a process.

While notices to affected consumers are required, an organization will also have to prepare notices to law enforcement, media responses, and ensure compliance with Florida Statute 817.5681 and other Florida and federal laws, such as Health Insurance Portability and Accountability Act (“HIPAA”) and its implementing regulations. Florida-based businesses that maintain data about the residents of other states must ensure familiarity and compliance with those state laws requiring breach notifications. Companies that conduct business in several states may want to have more standard responses to security breaches, as a majority of states have enacted security breach disclosure laws and these state laws are inconsistent in terms of definitions, deadlines, and penalties. Finally, all companies should be aware that the Stimulus Bill signed in February by President Obama sets forth new, farther-reaching federal breach notification requirements related to unsecured protected health information. These new requirements are applicable to all entities that are “covered entities” pursuant to the HIPAA and will generally apply in addition to the state law requirements. Although these new federal breach notification requirements are beyond the scope of this article, you can find a decision flow chart for determining whether notification is required under these new requirements by going to Trenam’s Health Law Newsletter under the publications tab at www.trenam.com. ■