COSMOS
Navigate the Compliance Universe

Compliance Today - January 2022
Breach notification: HIPAA is not the only law to worry about

By Marti Arvin


Marti Arvin

Marti Arvin (marti.arvin@comcast.net) is VP, Chief Compliance Officer, at Erlanger Health System in Chattanooga, TN.

Most healthcare compliance and privacy professionals have become familiar with the requirements of the Health Insurance Portability and Accountability Act (HIPAA) Breach Notification Rule. When a data compromise of protected health information (PHI) occurs, healthcare organizations have a process to evaluate the situation to determine whether notification to patients is required. However, it may be less common to have a process to evaluate obligations under state laws. Most states have some form of breach notification requirements when the personal individually identifiable information about an individual who is also a resident of the state is compromised. This may include both patient and nonpatient information. The increase of employees working remotely and more frequently living in a state that is different from the place they work may mean there are more instances where an organization holds information of residents from multiple states than in the past.

If an organization has a significant data compromise, it will likely be necessary to evaluate whether there are any obligations under state breach notification laws. This evaluation could get quite complex. State laws often apply when the data about a resident of the state is compromised, but many states exempt organizations or data covered by HIPAA. The state law could have requirements in addition to HIPAA. States may have varying definitions of what constitutes individually identifiable information. To fully evaluate the application of state breach notification laws, several steps must be taken.

Step 1: Assessing the data

Organizations will need to evaluate whose data was potentially affected and the status of the data. A determination will need to be made whether the potentially affected persons are patients, employees, visitors, contractors, or others. It will also be necessary to determine whether there are individuals involved for whom the organization might hold data in more than one capacity. For example, if the individual is an employee and a patient of the organization, there could be data affected for the person from the human resources department and some information from the individual's electronic health record.

Even though the data was about one person, the breach notification obligations might vary for each class of information under state breach notification laws. The PHI from the electronic health record might be exempted from state breach notification laws, but the human resources data might not be. If the organization is an institution of higher education, a security incident might involve PHI and data covered by the Family Educational Rights and Privacy Act (FERPA).[1] FERPA does not currently have any obligations regarding breach notification, but the data covered by FERPA may be subject to state laws. Compliance and privacy professionals also need to be aware there may be more than one state law that needs to be evaluated.

If the data compromise involves multiple data sources, there may also be a need to determine whether there is

duplicate data and/or multiple sources and types of data about the same individual. The organization may want to consider correlating the data by person, data elements, and source to help assess what laws might be applicable. This will also help when it comes to drafting the breach notification letters to individuals.