# Updated Illinois Data Breach Law Set to Take Effect Next Month

December 5, 2016 - The State of Illinois is making major changes to its data breach notification requirements on January 1st. The changes will redefine "personally identifiable information" (PII) to include a broad range of medical record information. That's the good news. The bad news is that the law doesn't allow private citizens to enforce their rights through legal means. Only the Illinois Attorney General can do that.

Tweet

(function() {
var s = document.createElement('SCRIPT'), s1 = document.getElementsByTagName('SCRIPT')[0];
s.type = 'text/javascript';
s.src = 'http://widgets.digg.com/buttons.js';
s1.parentNode.insertBefore(s, s1);
})();

(function() {
var po = document.createElement('script'); po.type = 'text/javascript'; po.async = true;
po.src = 'https://apis.google.com/js/plusone.js';
var s = document.getElementsByTagName('script')[0]; s.parentNode.insertBefore(po, s);
})();

The change in the state's law is significant. The updates mean that breaches medical information, health insurance information or policy numbers, diagnosed conditions and biometric information will all be considered PII. Any breach of this data can trigger the notification requirements of the law.

Companies affected by the law will be required to implement "reasonable security procedures" to protect their data. They will also be required to modify any third party contracts they have for data management or access to include this requirement.

The law does have some soft spots however. Enforcement is strictly up to the state. Individuals can't sue to enforce their rights. Furthermore, if encrypted data is stolen then no notification is required unless the encryption key is also breached.

The law doesn't just impact companies with a physical presence in Illinois. Any company that is serving customers in the state is impacted. This means that companies that supply medical devices via mail order or through the internet may be good examples of entities that will be impacted by the law. Online pharmacies are another example. Both types of company routinely collect, store and use insurance data as a part of their transaction process.
byJim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.
Follow me on Twitter:

Follow ACCESS