Massachusetts Data Security Regulations: Deadline Looms for Amending Service Provider Contracts

By Cynthia Larose on February 10th, 2012

Just a reminder that **March 1** is an important deadline with respect to the Massachusetts data privacy and security regulations (the "Regulations"). As a refresher, the Regulations require all entities that "own or license" personal information of Massachusetts residents — wherever the entity is located — to comply with provisions requiring specific administrative, physical and technical safeguards in respect of the personal information. To reduce the risk of data breaches involving third-party service providers who will have access to personal information in some way, the Regulations require companies covered by the Regulations to take reasonable measures to select vendors capable of "maintaining appropriate security measures to protect such personal information consistent with [the] regulations and any applicable federal regulations." Furthermore, the Regulations mandate that companies **contractually require** their service providers to safeguard personal information in accordance with the Massachusetts regulations and applicable federal requirements. Regardless of location, an entity must comply if it receives, stores, maintains, processes, or otherwise has access to personal information of Massachusetts residents in connection with the provision of goods and services or in connection with employment. Because the Regulations contain such broad definitions for terms such as "own and license," most service providers – from your payroll provider to your e-commerce hosting provider – are likely subject to this requirement.

The contract provision includes a grandfather clause, providing that all contracts entered into before March 1, 2010 are exempt from complying with this requirement until March 1, 2012. By March 1, 2012, companies that own or license PI of Massachusetts residents must ensure that pre-March 1, 2010 contracts with third party service providers are amended to incorporate appropriate contractual requirements. Regardless, service provider contracts entered into after the March 1, 2010 effective date of the Massachusetts regulations have been and continue to be required to contain such a contractual representation of compliance.

If your company relies on service providers to receive, store, process or otherwise access personal information of Massachusetts residents, you should be ensuring that those service provider contracts contain a representation that appropriate administrative, physical and technical safeguards are maintained to protect the personal information. Letters from service providers "certifying" that they are in compliance with 201 CMR 17 are not sufficient to meet the requirements of the Regulations if they do not specifically act as an amendment to whatever agreement you have in place with a service provider.