PARTRIDGE SNOW & HAHN LLP
COUNSELORS AT LAW

Is your "Written Information Security Program" Ready for the March 1, 2010 Deadline?

February 2010

Michael A. Gamboli, Esq.

Mass. General Laws Chapter 93H requires every company that maintains or stores personal information ("PI") of a resident of the Commonwealth of Massachusetts to provide extensive notification to authorities if PI is ever compromised. In order to prevent PI from ever being compromised, new regulations promulgated under this statute now require companies to develop, implement and maintain a comprehensive "Written Information Security Program" ("Program") to protect PI. The deadline for putting a Program in place is *March 1, 2010*. The level of detail required of a Program is generally considered excessive, which likely accounts for the fact that the deadline for compliance has been extended three times. However, further extension of the March 1, 2010 deadline is not anticipated.

Your company's written Program must, among other things, designate one or more employees to maintain the Program; identify and assess internal and external risks to the security of electronic, paper, or other records containing PI; develop security policies for employees relating to storage, access and transportation of PI; set forth secure user protocols for computer and wireless device access and encryption of electronic records; require the execution of written contracts with third party service providers capable of protecting PI; ensure for the regular monitoring and updating of the Program; and provide for the documentation of responsive actions to be taken in connection with any incident involving a breach of the security of PI.

Importantly, a Program is required for every company that maintains personal information about an individual living in the Commonwealth of Massachusetts regardless of whether the company is located or has any offices in Massachusetts. The good news is that the final regulations include a provision indicating that the safeguards put into place by the Program should be appropriate to the size, scope and type of your business, the amount of resources available, the amount of PI data at issue, and the need for security of customer and employee information.

Companies are urged to review the new regulations (201 CMR 17.00) and to make sure that their organization is fully compliant by March 1, 2010.

If you have questions about your program's compliance with the new regulations (201 CMR 17.00) or the Breach Notificaton Law (M.G.L. Ch. 93H) you are welcome to contact
Mr. Gamboli, mag@psh.com, 401-861-8255.

Click here for information on 201 CMR 17.00