

CLIENT ALERT: AUGUST 23, 2010

NON-PROFITS AND THE MASSACHUSETTS DATA PRIVACY REGULATIONS

The Massachusetts data privacy regulations (201 CMR 17.00 et seq.) specify how businesses and non-profits handle and store “personal information” of Massachusetts residents, as defined in the data privacy regulations, including social security numbers, credit card information, bank account numbers and drivers’ license numbers. If your organization handles or stores any personal information, your organization will need to comply with the new regulations. For example, your organization must comply with these regulations if you collect donors’ credit card information in connection with fundraising or employees’ bank account information in connection with payroll.

Under the new regulations, your organization must satisfy the following requirements:

- You must implement a comprehensive written information security program (now commonly referred to as a “WISP”) that complies with the regulations. This program can be tailored based on the size and scope of your organization and the amount of personal information to be handled and stored.
- Your WISP should identify which employees are responsible for implementation. In addition, all employees should be trained to handle, store and destroy personal information appropriately and to take prescribed actions if a security breach occurs. In addition, your WISP should spell out the consequences for non-compliance.
- Employees should only have access to personal information on a “need to know” basis.
- If personal information is stored in hard copy form, physical access to the materials containing personal information should be restricted.
- To the extent technically feasible, you must ensure that personal information is encrypted before it is (i) emailed or transmitted wirelessly or (ii) stored on laptops or other portable devices.
- If you hire outside contractors (such as fundraisers) who may be handling personal information, you will need to ensure that these contractors keep all personal information secure, and your contracts with these parties should require them to comply with the new regulations.

If your organization fails to comply with the new regulations and a security breach occurs, this could lead to negative publicity, impaired donor relationships, investigations by the Massachusetts Attorney General’s Office and/or litigation.

Please contact Sheryl Howard at 617-482-7211 or showard@kb-law.com, if you have any questions or would like assistance preparing a WISP.

A copy of the regulations is available at:

<http://www.mass.gov/Eoca/docs/idtheft/201CMR1700reg.pdf>

For additional information regarding the Massachusetts Data Privacy Regulations, see:

<http://www.kb-law.com/articles/documents/DataSecurityRegulations.pdf>