Privacy and Security Alert: Tick-Tock: It's February 1 - The Countdown to Compliance with the Massachusetts Data Security Regulations Has Begun!

2/1/2010

By Cynthia J. Larose

As we've been discussing since January 2008 (please see our alerts dated January 29, 2008, October 2, 2008, October 31, 2008, January 30, 2009, August 17, 2009 and August 19, 2009), entities that own, license, access or process the personal information of Massachusetts residents are coming down to the wire for implementing the data security standards in 201 CMR 17.00, *Standards for the Protection of Personal Information of Residents of the Commonwealth,* otherwise known as the Data Security Regulations. The compliance deadline is March 1st.

For the procrastinators among you, it appears reasonably certain (after conversations with the Massachusetts Office of Consumer Affairs and Business Regulation) that the March 1st deadline will hold and businesses covered by the Data Security Regulations will be expected to have conducted the required risk assessment and to have implemented the required security measures and information security plan.

The Commonwealth has provided some resources on its website, including an FAQ document and a basic template to assist with development of an information security plan. These resources are a good starting point, but should not be considered a complete (or compliant) security plan. Because the Data Security Regulations specifically require that the plan be risk-based and specific to your business, adoption of a "canned" information security plan creates considerable risk that you have not identified the appropriate measures for your company.

Top Five Misapprehensions about Compliance with the Regulations

5. "We are a not-for-profit (charitable organization, etc.), so the Data Security Regulations do not apply to us."

   Unless you are a municipality or state governmental entity, the Data Security Regulations **do** apply to your organization. You likely have personal information of your donors, and you certainly have personal information of your employees (and perhaps volunteers). All of this is covered by the Data Security Regulations when the personal information in your hands.

4. "My business does not keep any personal information. We process it in the course of our

service arrangements with customers, but do not retain it, so we don't need to develop an information security plan."

The Data Security Regulations apply to any entity that "owns or licenses, maintains, **processes**, or otherwise has access to personal information in connection with the provision of goods or services…." and such entities are required to develop written information security plans that, **at a minimum**, meet the standards in the Data Security Regulations. Your customers will be looking for it. See the requirement in Section 17.03(f) relating to the required oversight of service providers.

3. "We are required to comply with HIPAA (or Gramm-Leach-Bliley, or FERPA, or any other state or federal data privacy regulations), so we do not have to separately comply with the Data Security Regulations."

   They may overlap, but compliance with the others does not preempt your requirements to comply with the Data Security Regulations. You should be evaluating your current data security policies and procedures under any other regulatory environment to ensure that the policies do not conflict and create barriers to compliance with the Data Security Regulations. Section 17.02(1)(d) specifically states that "[t]he safeguards contained in such program must be consistent with the safeguards for protection of personal information and information of a similar character set forth in any state or federal regulations by which the person who owns or licenses such information may be regulated."

2. "My business does not collect any credit card or consumer data, so the Data Security Regulations do not apply to me."

   The Regulations specifically apply to personal information of Massachusetts residents collected in connection with employment. Therefore, if you have Massachusetts employees, the Data Security Regulations apply to you.

And the #1 misapprehension we hear about compliance with the Data Security Regulations:

1. "I'm located outside Massachusetts, so the Data Security Regulations do not apply to me."

   See the response to #2. Also, if you have Massachusetts customers and have personal information about those customers, the Data Security Regulations apply to that information and the safeguarding of it, whether you are physically located in Massachusetts or elsewhere.

* * *

For more information and up-to-date compliance tips, please visit the Mintz Levin Privacy *MATTERS* Blawg. If you need assistance with a risk assessment, or development of an information security policy, please contact a member of our Privacy and Security Group, or your Mintz Levin attorney.

For assistance in this area please contact one of the attorneys listed below or any member of your Mintz Levin client service team.

Cynthia J. Larose, CIPP
(617) 348-1732
CLarose@mintz.com

Dianne J. Bourque
(617) 348-1614
DBourque@mintz.com

Elissa Flynn-Poppey
(617) 348-1868
EFlynn-Poppey@mintz.com

Haydon A. Keitner
(617) 348-4456
HAKeitner@mintz.com

Julia M. Siripurapu
(617) 348-3039
JSiripurapu@mintz.com