

## **Massachusetts MA 201 CMR 17.00 – Best Practice Guidance on How to Comply**

MA 201 CMR 17.00 has been in the news for the last 18 months. Whilst no one was sure when it would come into effect, it has now been confirmed that the Massachusetts information security regulations, entitled “Standards for the Protection of Personal Information of Residents of the Commonwealth,” also known as “MA 201.17” will take effect on March 1, 2010. The regulations apply to entities that own or license personal information about Massachusetts residents. It is important to note that rules apply to all entities, wherever located, with “personal information” of Massachusetts residents.

For most organizations this is yet another complex and hard to grasp piece of law to comply with. Why has Massachusetts decided to design and enact MA 201? What is meant by personal information? How are you supposed to safeguard it? What are the best practices to ensure compliance and what are the steps you need to take to achieve and maintain compliance with MA 201? What is the upside of MA 201 for your business if any?

### **1. Why has Massachusetts decided to design and enact MA 201?**

There has been a significant number of high-profile data breach cases in the US over the past few years. For instance, in 2007 TJX Companies Inc., the global conglomerate that includes T.J. Maxx, T.K. Maxx, Marshalls and Winners, lost at least 45 million credit cards after systems were penetrated by hackers. In 2009 Networks at Heartland Payment Systems were hacked, exposing data on 130 million credit card users and, also in 2009, the Network Solutions data security breach exposes a half-million credit card numbers. In addition, breaches must be reported in 45 US States and Federal Breach Disclosure law is on its way. It is worth noting that the State of Massachusetts requires that breached entities report data breaches to the Massachusetts Office of Consumer Affairs and Business Regulation.

However, security experts always warn that breach notification alone is insufficient. This is a re-active measure to ensure that crisis management procedures are put in place to contain the issue, to inform citizens that their data has been or may have been compromised and restore confidence in the markets after an incident has taken place. What is required is a more pro-active data protection approach with focus on protecting personal information before incidents happen. This is not meant to replace Data Breach Protection but rather to complement it.

It is also worth noting that regulators determined that data in transit or on portable devices is most at risk and that several US States such as Nevada already require that such data be subject to additional levels of protection, such as encryption and associated policies. Nevada even requires designated organizations to comply with industry standards such as PCI DSS (Payment Card Industry Security Standards) which sets out technical and logical controls around cardholder data protection.

Massachusetts is the first to take this pro-active approach in the US and it seems that it is determined to ensure that personal information is adequately protected. Litigation and enforcement will be driven by the Massachusetts Attorney General. Massachusetts law requires notice to the Attorney General and OCABR of any breach, in addition to affected consumers and the Attorney General likely is to wish to investigate based on breach reports. At this stage there are no clear private right of action or penalties regarding enforcement however one thing is for sure, MA 201 CMR will be enforced.

## 2. What is meant by personal information?

“Personal information” is defined as a combination of a resident’s first and last name and Social Security number, driver’s license or state ID number, or financial account number or payment card number that permits access to the individual’s financial account.<sup>i</sup> This is key to understanding the type of data covered by MA 201.

## 3. How are you supposed to safeguard it?

One needs to understand the type of safeguards required to comply. Organizations must have a mix of physical and logical safeguards as well as policies and procedures and awareness training for staff. This will involve the following tasks:

- a) Design and promotion of a written Information Security Program (“WISP”)
- b) Asset inventory and asset classification process for data & physical assets
- c) Risk assessment process, ideally involving a risk treatment procedure
- d) Contracts to govern 3<sup>rd</sup> Party management (e.g. suppliers, contractors)
- e) Identity and access management policies and associated log trails
- f) Incident Response Plan
- g) Encryption (for specific data)
- h) Configuration & Vulnerability Management Policy

There has been a lot of talk about the Written Information Security program (“WISP”) that businesses must put in place. Broadly speaking this covers policies and procedures allowing organizations to inventory and classify their physical and logical assets, an acceptable usage policy governing how corporate communication tools used to transmit, store or process personal information can be used by staff – this includes e-mail, Internet, IM, social networking, USB memory keys, etc. It also requires an Incident Response Plan, an access control policy, an education program for staff a disciplinary procedure for non-compliant staff, a process for managing accounts and rights of terminated or leaving staff.

It is important to realize that the WISP must contain “administrative, technical and physical safeguards” that are “appropriate” to the Entity’s size, scope and type of business, Entity’s resources, amount of stored data, need for security and confidentiality of both consumer and employee information.<sup>ii</sup> It is also relevant to note that the WISP must also allow the entity to comply with applicable State and federal laws.

One key element of MA 201.17 is to designate a Data Security Coordinator who is an employee(s) responsible to develop security policies for employees, Including keeping, transporting and accessing records and data off-site. This is most likely going to be a Chief Security Officer or Chief Compliance Officer, C-Level person or senior manager.

### **Focus on technical security solutions required to comply:**

In terms of technical controls, entities must establish and maintain a “security system” for their computer systems and network. This includes, but is not limited to, the following technical solutions:

- Firewalls
- Security Patching (whether installed manually or through an automated solution)
- Anti-Virus and Malware protection software
- “If technically feasible laptops and other portable devices must be encrypted, as must all records and files transmitted over public networks
- All computer systems must be monitored for unauthorized use of or access to personal information”
- A password policy and protocol for control of User IDs and identifiers must also be in place
- Vulnerability Management solutions must be in place so as to ensure that all systems are properly patched and secure.

In addition, entities must demonstrate that they restrict physical access (with locks), prevent access to personal information by former employees ideally addressed by a leaver’s policy and an associated check list to ensure that all corporate communication media devices such as laptops, PDAs, phones, USB keys are returned and analyzed for unusual activity. If such activity is detected then the incident response plan is to be launched.

### **Continuous Compliance aspect of MA 201.17:**

Regular monitoring must be enforced to ensure the program is operating, Should it not or should technical solutions need be upgraded, the entity needs to take corrective action. The security measures put in place by the entity as well as the WISP must be reviewed annually or whenever there is a material change in business.

### **Focus on Vulnerability Management:**

Whilst MA 201.17 does not specifically require entities to use specific type of vulnerability management solutions, it does require entities to ensure that all systems containing personal information are protected and that “there must be reasonably up-to-date versions of system security agent software which must include malware protection and reasonably up-to-date patches and anti-virus definitions”.

This is best achieved by using vulnerability management software that scans IP addresses for known vulnerabilities and provides a view of what hackers would see from the outside in and provides advice on remediation work to be carried out.

### **Focus on Education and Training:**

Under MA 201.17 entities must provide security awareness training to all staff and must ensure that they receive a copy of the WISP and acknowledge in writing that they have received the copy. In addition, it is worth noting that staff employment contracts must be written in such a way that they have to comply with provisions of the WISP.

This is based achieved through face-to-face of eLearning training sessions covering the basics of security. Ideally businesses will want to be able to distribute the WISP (or attach the WISP in the case of eLearning) and keep track of written or electronic acknowledgement of receipt of the WISP.

#### **Focus on Third Parties Management:**

As with most legal and industry security frameworks, MA 201.17 puts great emphasis on managing third party involved in the business of affected entities. Specifically, MA 201.17 makes it mandatory for entities to ensure that no third party engaged by them can become the “weakest” security link in the trust chain put in place under the WISP such that a third party does not become a risk to the overall security posture of the business.

As such, “covered entities to take steps to select and retain service providers that are capable of appropriately safeguarding personal information. Covered entities must contractually require their service providers to safeguard personal information [...] provided, however, that service provider contracts entered into no later than March 1, 2010, are exempt from complying with this requirement until March 1, 2012”.<sup>iii</sup>

#### **4. What are the best practices to ensure compliance and what are the steps you need to take to achieve and maintain compliance with MA 201?**

- I. There are a number of steps to follow.
- II. The first thing is to Identify all records used to store personal information and assess associated risks to personal information
- III. This must include both internal and external risks
- IV. The next step is to evaluate (and improve) safeguards, both at logical (IT) and at a physical levels.
- V. Employee training and compliance

It also key that restrictions upon physical access to records containing personal information are implemented and that storage of such records and data only be done in locked facilities with secured storage areas.

Whilst the key person looking after the WISP has to be the Data Security Coordinator, organizations may be advised to create a team including IT, HR, Legal, Compliance and Operations to ensure that all legal, commercial and operational aspects of data security are covered in the WISP. This team must then ensure that it regularly reviews existing policies, regularly reassess risks as well as internal and external threats.

As with any type of legal or industry frameworks businesses are advised to reflect on how they ne able to reduce the scope of applicability of MA 201.17. Ma 201.17 requires protection around personal information so does your business really need to collect, store or process the amount of personal information it deals with? Is there any way that personal information amounts cane be reduced? To ascertain if this can be done organizations will need to map data flows in electronic and paper formats that include personal information and should also consider limiting the collection of personal information and restrict access to those with a need to know.

On an ongoing basis, entities need to continually work on identifying new internal and external risks and on monitoring and improving the effectiveness of current safeguards. It is also key to ensure that employees are trained regularly, at least once a year and upon hire. Systems need to be regularly updated with specific focus on firewall protection and malware and virus protection.

Finally, as far as Third party vendor contracts are concerned, entities need to be mindful to incorporate clauses in or work out amendments to vendor agreements and confirm that vendors will implement and maintain appropriate measures to be in line with those put in place by the entity. This is mostly done through the use of strong third party contract management policies.

## **5. Upside**

It is clear that Massachusetts 201 CMR 17.00 can be seen by covered entities as a burden in terms of operational duties, time and effort. However it is worth acknowledging that earlier versions were putting even stricter rules for all entities. The current MA 201.17 states that “duty to protect personal information through information security program modified to allow the administrative, technical and physical safeguards to be “appropriate” to Size, scope and type of business, Amount of resources and data, Need for security and confidentiality of the data”. This should be welcome by covered entities as it provides them with more flexibility especially for small businesses.

In fact, small businesses would be advised to read the “Small Business Guide: Formulating A Comprehensive Written Information Security Program”<sup>iv</sup> which provides a lot of very insightful and useful information on how to comply with MA 201.17.

The main upside of MA 201.17 is that it is fully in line with security best practices and compliance with it will bring you a long way towards compliance with other legal and industry frameworks such as Data Breach Notification laws, ISO 27001, Payment card Industry Data Security Standard (PCI DSS) and vice versa.

It is also worth noting that the pro-active nature of MA 201.17, as opposed to Data Breach Notification laws which entities are more widely in compliance with, aligns organizations closer to the European Data Protection Directive which is the basis for most data protection legislation in the EU so if your organization is also doing business in the EU, then MA 201.17 compliance will make it easier for you to comply with EU Data Protection Mandates.

The main thing to keep in mind is that every requirement of MA 201.17 is something that every organization needs to be doing to protect personal information. It is simply best practice and common sense to ensure that sensitive data is protected by physical and logical safeguards and based on a risk assessment and associated risk treatment which takes into account every data and IT asset in place. This is simply best practice.

---

<sup>i</sup> <http://www.huntonprivacyblog.com/2010/02/articles/enforcement-1/massachusetts-information-security-regulations-take-effect-on-march-1-2010/index.html>

<sup>ii</sup> SecureWorld Spotlight, 201 CMR 17.00: A Litigator's Perspective, Goodwin Procter.

<sup>iii</sup> <http://www.huntonprivacyblog.com/2010/02/articles/enforcement-1/massachusetts-information-security-regulations-take-effect-on-march-1-2010/index.html>

<sup>iv</sup> [http://www.mass.gov/Eoca/docs/idtheft/sec\\_plan\\_smallbiz\\_guide.pdf](http://www.mass.gov/Eoca/docs/idtheft/sec_plan_smallbiz_guide.pdf)

#### About the author:

Mathieu Gorge is the CEO and founder of VigiTrust. He has been in the security industry for the past 10 years. In 2003 Mathieu identified a gap in the market to provide pro-active consultancy services around key legal aspects of corporate security such as compliance with international data protection legislation as well as industry security frameworks such as PCI DSS and ISO 27001. He is a regular speaker at international security conferences (RSA, ENISA, ISACA) and a well respected figure in the security industry in North America and in EMEA. He may be reached at [mathieu.gorge@vigitrust.com](mailto:mathieu.gorge@vigitrust.com).