

A New Massachusetts Law Requires Businesses to have a Written Information Security Plan (WISP)



by Anna DeSimone

Pursuant to the authority granted under M.G.L. c 93H, the Massachusetts Office of Consumer Affairs and Business Regulation retroactively promulgated 201 CMR 17:00, a law requiring all financial organizations to have a written plan to protect personal consumer information. On February 1, 2010, Bulletin No. 2010-02 was issued by the Office of consumer Affairs and Business Regulation setting forth the regulation effective March 1, 2010.

The plan is referred to as the *Written Information Security Program (WISP)* and applies to any business entity that has access to confidential consumer information of any resident of the Commonwealth of Massachusetts.

WISP is a comprehensive program that defines security standards for computers and handling of consumer information. The law applies to all business entities that own, license, store or maintain certain personal information.

Personal Information consists of a Massachusetts resident's first name and last name (or) first initial and last name in combination with *any* of the following:

- Social Security Number
- Driver's License Number / or State-issued Identification Card Number
- Financial Account Number
- Debit or Credit Card Number (with or without security/access codes/passwords/pins)

Not Applicable Personal Information includes government records or information that is lawfully obtained and made available to the general public.

Required Elements of the WISP Program:

The Written Information Security Program must provide administrative, technical and physical safeguards for personal information under 201 CMR 17.00. This states that all businesses have a duty to protect the information of a Massachusetts resident that has been received by the company in connection with employment or the provision of goods or services – this would apply to the origination, processing, approval, funding, settlement or servicing of a consumer's mortgage.

If personal information of a consumer is electronically stored or transmitted, the security program must cover computers and portable and/or wireless devices. The WISP must be appropriate to the size, scope and type of business, available resources, the amount of stored data and the need for security and confidentiality of consumer and employee information.

The WISP program should address a wide range of matters that include, but are not limited to:

- Analysis of the reasonably foreseeable risks to the security, confidentiality and integrity of records, in any form, that contain personal information, of the effectiveness of any current safeguards for limiting those risks, and of the need to develop improved safeguards.

This article first appeared in the AllRegs Weekly Digest and may be viewed in its original format at http://www.allregs.com/ealerts/updates100211_WISP-MA.htm.

- Policies and procedures relating to employee training on the importance of the WISP, its specific requirements, the consequences of failure to comply with those requirements, and prevention of access by former employees.
- For paper records, provisions for secure storage of materials containing personal information, including restrictions on physical access to such records and, for electronic records, control measures that restrict access and include secure user authentication protocols.
- Encryption of personal information that is stored on computers, laptops or other portable devices or is transmitted across public networks or transmitted wirelessly.
- Provisions to ensure that any electronic records system that is connected to the internet includes firewall protection and operating system security patches, that security software includes malware protections and virus definitions, and that all these programs are reasonably current as of March 1, 2010 and will be updated on a regular basis thereafter.
- Oversight of third-party service providers who have access to personal information, including a process to select and retain service providers that are able to maintain appropriate security measures consistent with 201 CMR 17.00.
- Regular monitoring to ensure that the WISP operates effectively to protect both paper and electronic records, to detect any unauthorized use of or access to personal information, and to identify any areas where upgraded safeguards are needed.
- Review of the WISP's scope at least annually, and whenever there is a material change in business practices that may reasonably implicate the protection of personal information.
- Documentation of responses to any breach of security and of any actions taken thereafter to change practices relating to the protection of personal information.

On February 1, 2010, the Massachusetts Office of Consumer Affairs and Business Regulation enacted a new law requiring businesses with access to personal information to have a Written Information Security Program (WISP). Effective March 1, 2010, this new law applies to any business with access to personal consumer information belonging to any resident of the Commonwealth of Massachusetts.

The plan must outline the company's overall corporate-wide program to detect, prevent, and mitigate information security breaches. Do you have your plan in place?

If not, let AllRegs do all of the work for you with our **Electronic Security Plan [Massachusetts] Policy Manual**. This 19-page, customizable policy and procedure manual includes everything your company needs to stay compliant with Massachusetts General Law 93H 201 CMR 17.00. From computer system and network requirements and firewall procedures, to prohibited activities and monitoring, the Electronic Security Plan [Massachusetts] Policy Manual satisfies all necessary requirements of the Written Information Security Program. Turn our plan into *your* plan with AllRegs' Electronic Security Plan [Massachusetts] Policy Manual.

To learn more visit: http://www.allregs.com/products/products.aspx?l=ppm_espMA.htm

*Anna DeSimone is President of Bankers Advisory, Inc., Belmont, Massachusetts. She authors Policy Manual Templates for AllRegs and her company authors and updates AllRegs' State Rules Matrices, Permissible Fee Matrix and Compliance Checklists for 50 states.

This article first appeared in the AllRegs Weekly Digest and may be viewed in its original format at http://www.allregs.com/ealerts/updates100211_WISP-MA.htm.

Copyright © 2009 AllRegs. Reprinted with permission from AllRegs, <http://www.allregs.com>.



Disclaimer: The information presented in this article represents the opinion of the author and not that of AllRegs. This article is not meant to be nor should it be construed as advice of legal counsel. The applicability of the information contained herein will vary based on the nature of each lending institution's business, under what law it was created, and its loan products and procedures. Readers are strongly urged to consult with their legal counsel and/or contact local counsel as appropriate in the various states and jurisdictions to determine the applicability of the materials contained herein to the specific facts and circumstances of each organization's programs and products and to identify other law applicable to its business operations. The information contained herein was not reviewed or approved by counsel in the respective jurisdictions.

This article first appeared in the AllRegs Weekly Digest and may be viewed in its original format at http://www.allregs.com/ealerts/updates100211_WISP-MA.htm.