

2010-02 Compliance with 201 CMR 17:00, Standards for the Protection of Personal Information of Residents of the Commonwealth

TO: All Individuals and Entities Licensed by the Division of Insurance
FROM: Joseph G. Murphy, Acting Commissioner of Insurance
DATE: February 1, 2010
**RE: Compliance with 201 CMR 17:00, Standards for the Protection of
Personal Information of Residents of the Commonwealth**

The Office of Consumer Affairs and Business Regulation, pursuant to the authority granted to it by G.L. c. 93H, in November 2009 promulgated 201 CMR 17:00, a regulation setting standards for the protection of personal information of Massachusetts residents. The Division of Insurance reminds all of its licensees about their obligations under this regulation and the March 1, 2010 deadline for full compliance.

Any person that receives, stores, maintains, processes or otherwise has access to personal information acquired in connection with employment or with the provision of goods or services to a Massachusetts resident has a duty to protect that information. A “person,” for purposes of the regulation, may be an individual, corporation, association, partnership or other legal entity. Personal information includes a surname, together with a first name or initial, in combination with one or more of the following three data elements pertaining to that person: Social Security Number; driver’s license or state-issued identification card number; or financial account or credit or debit card number, with or without any other data element, such as a code, password, or PIN, that would permit access to the person’s financial account.

The duty includes the requirement that the person develops and maintain a comprehensive written information security program (“WISP”) to safeguard such information. If the person electronically stores or transmits personal information, the WISP must include a security system covering the person’s computers and any portable and/or wireless devices. Safeguards should be appropriate to the size, scope and type of the person’s business, to the person’s available resources, to the amount of stored data and to the need for security and confidentiality of consumer and employee information. They must be consistent with safeguards for the protection of personal information, and information of a similar character, that are set out in any state or federal regulations that apply to the person.

A WISP must provide administrative, technical and physical safeguards for personal

information under 201 CMR 17.00. It must address a wide range of matters that include, but are not limited to:

- Designation of the individuals who will oversee and maintain the WISP;
- 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;
- 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; and
- Documentation of responses to any breach of security and of any actions taken thereafter to change practices relating to the protection of personal information.

A complete copy of 201 MR 17.00 may be found at:

<http://www.mass.gov/Eoca/docs/idtheft/201CMR1700reg.pdf>. Additional information may be found at the Office of Consumer Affairs and Business Regulation's website, following this link:

<http://www.mass.gov/?pageID=ocatopic&L=3&L0=Home&L1=Business&L2=Identity+Theft&sid=Eoca>