INFORMATION SECURITY: A BUSINESS NECESSITY FOR MEDIATORS

By William M. Driscoll

Perhaps the greatest myth of 2009 is the date by which businesses must protect personal information of residents of the Commonwealth. The "Standards" released by the Office of Consumer Affairs and Business Regulation carry an effective date of January 1, 2010. However, the enabling law, Massachusetts General Laws chapter 94H, went into effect in 2007. Why the confusion?

History For years the media has publicized instances of identity theft — primarily focusing upon large corporations failing to comply with federal law. Forty-four States and the District of Columbia have now enacted Security Breach laws for the protection of "personal information." In Massachusetts and elsewhere, the law related to information security, data protection, and privacy has instilled stronger duties upon business owners and boards of directors.

The first of these duties is that of data governance — the ongoing management of risk regarding the safeguarding of information within the purview of the business, from inception to destruction. Data governance charges the business or organization with the responsibility for physical, procedural, and technical measures to safeguard personal information. The risks associated include those related to the collection, use, disclosure, transfer, modification, and destruction of sensitive information.

The second of these duties is the fiduciary duty of care to safeguard the integrity and confidentiality of sensitive information. Guidance for the safeguarding of information is rapidly emerging from legal compliance requirements. One requirement of the fiduciary duty is that of mandatory employee training so as to ensure that the actual business operating procedures are commensurate with the written security policies and procedures. Training is crucial as the business owner and board of directors, if any, is ultimately responsible!

The marketing message that mediators should convey to their clients is, "We care about your privacy and we work hard to protect it."

Massachusetts Law (effective 2007) The Commonwealth of Massachusetts legally obligates businesses holding personal information about a resident of the Commonwealth to protect that information. The guiding law is Massachusetts General Laws chapters 93H and 93I — both effective in 2007. To meet the minimum requirements of the law and to avoid negligent release of personal information each business must draft a substantial and substantive written document outlining its

Information Security Program; its information protection policies and procedures; training and disciplinary procedures. The business of mediation is not exempt!

The marketing message that mediators should convey to their clients is, "We care about your privacy and we work hard to protect it."

Massachusetts General Laws, chapter 93H (Security Breaches) was enacted in 2007. The law requires businesses to protect all "personal information" of residents of the Commonwealth in whatever forms — whether paper, digital, or other. Violations of the law may result in substantial monetary fines and lawsuits. The Standards for protection (201 CMR 17.00) have an effective date of January 1, 2010. However, the law is currently enforceable as the standards do exist. In addition there are federal, state, and local laws; industry standards; professional standards; and common sense.

Massachusetts General Laws, chapter 93I (Dispositions and Destruction of Records) was also enacted in 2007. It requires the protection of "personal information" of all residents of the Commonwealth through standards of destruction for such records.
Data destruction is media dependent. Paper documents containing personal information: redacting, burning, pulverizing, or shredding so that personal data cannot practicably be read or reconstructed. Non-Paper documents and electronic media containing personal information: destruction or erasure so that personal data cannot practicably be read or reconstructed. The "Standards" for the disposition and destruction of records are embedded within the law and therefore, clearly stated as of 2007.

How is "Personal Information" defined?
Personal Information is defined by statute in M.G.L. c. 93H: A resident's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident:

(a) Social Security number;
(b) Driver's license number or state-issued identification card number; or
(c) Financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account; provided, however, that "Personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

However, within M.G.L. c. 93I, the definition of "Personal Information" modifies paragraph (c) and adds paragraph (d), as follows:

(c) Financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password that would permit access to a resident's financial account; or
(d) A biometric indicator.

Why is this important? Because the "Standards" authorized under M.G.L. c. 93H include requirements for the destruction of personal information. However, those "Standards" do not comply with M.G.L. c. 93I. To be compliant under the law, the sum of the laws must be dealt with together!

Does this end the definition of personal information? No. In fact, each state with a law protecting personal information of its residents may define "Personal Information" differently and may apply its law to businesses interacting with its residents — even if they do not have a physical location within that State's borders. As a result, businesses within the commonwealth may desire to extend the definition of "Personal Information" to include information protected under other jurisdictions, or for other business reasons. After all, the law is only a minimum standard of care upon which to comply.

The Duty to Report Massachusetts General Laws chapter 93H, sections 3-5 place upon the business the burden of reporting known security breaches and unauthorized use of personal information. Notice shall be provided as soon as practicable and without unreasonable delay when the business:

(1) Knows or has reason to know of a breach of security, or,
(2) When the business knows of or has reason to know that the personal information of such resident was acquired or used by an unauthorized persona or used for an unauthorized purpose.

In fact, the business is charged with the duty of identifying breaches in security and unauthorized use of personal information. The business is legally obligated to bring such events to the attention of the State! The content of the notice must contain:

(1) A detailed description of the nature and circumstances of the breach, release, or use;
(2) The number of Massachusetts residents affected;

Investing in preventative measures now will pay-off later.

(3) The steps already taken relative to the incident;
(4) Subsequent steps intended to be taken; and,
(5) Status regarding law enforcement investigation, if any.

What is Required of a Written Information Security Program? The requirements of a Written Information Security Program (the "WISP") are described within M.G.L. c. 93H, § 2:

(1) To safeguard the personal information of residents of the Commonwealth; and,
(2) To remain consistent with the safeguards for protection or personal information set forth in federal regulations by which the business is regulated.
To achieve the requisite level of safeguards, each business — regardless of size — is charged with the responsibility to:
(1) Insure the security and confidentiality of customer information in a manner fully consistent with industry standards;
(2) Protect against anticipated threats or hazards to the security or integrity of such information; and,
(3) Protect against unauthorized access to or use of such information that may result in substantial harm or inconvenience to any customer.

To accomplish these goals, certain policies and procedures regarding administrative, technical, and physical methods must be incorporated into the "WISP." It is critical to ensure that the actual business practices of the business are commensurate with the business' WISP! Because each business operates based upon the unique "personality" of its owner(s), it is critical to recognize that there is not one "WISP" that will cover multiple businesses! Businesses trying to adopt another business' WISP as their own will likely encounter problems. The result may not reflect the actual business practices and a deceptive business practice may result.

Conclusion The time to act is now! The law regarding the safeguarding and disposal of personal information has been enforceable since 2007. Do not be lulled into a feeling of complacency until January 1, 2010 — the effective date of the Commonwealth's "Standards" guideline. Infractions of the law are subject to existing standards.

Prepare a Written Information Security Program ("WISP") and ensure your business practices comply with the written plan. Enlist the assistance of an information security and data protection professional to assist you in your efforts, for review, or for auditing your Program. Investing in preventative measures now will pay-off later. Remember, the cost of non-compliance is high!

William M. Driscoll, M.S., J.D. is a collaborative attorney, mediator, and litigator engaged in the practice of Information Security, Data Protection, and Privacy Law as well as Divorce and Family Law. Bill's practice is located in Chelmsford, and he invites you to visit his web site (www.DriscollEsq.com) or to email questions to wmd@DriscollEsq.com.