CLIENT ALERT: September 24, 2008

LONG-AWAITED REGULATIONS IMPLEMENTING CHAPTER 93H MANDATE DOCUMENT RETENTION PLANS AND DATA ENCRYPTION BY JANUARY 1, 2009

On Friday, September 19, 2008, the Office of Consumer Affairs and Business Regulation ("OCABR") promulgated final regulations pursuant to Chapter 93H of the General Laws governing the ways in which businesses must store and protect personal information about Massachusetts residents. Both for-profit companies and non-profit organizations that own, license, maintain, or store personal information must create and implement a document retention plan, referred to in the regulations as a comprehensive information security program ("CISP"), containing at least twenty different elements, including:

- mandatory encryption of personal information that is transmitted wirelessly or stored on laptops or other portable devices (note: this is a new provision not included in the proposed regulations issued last year);
- restrictions on physical access to materials containing personal information;
- user authentication protocols;
- mandating that contracts with third party service providers address data security protocols and safeguards;
- policies governing data access and use outside of the business premises (including, for example, employees who telecommute); and
- disciplinary measures for personnel who violate the terms of the CISP.

Contrary to the plain language of Chapter 93H as described in our initial client alert on this subject, according to the General Counsel for the OCABR, your company or organization must comply with these requirements regardless of any duty to comply with other state or federal laws governing record retention or data security, such as Sarbanes-Oxley, HIPAA, or FERPA.

Notably, since the enactment of Chapter 93H, approximately 40% of the security breach reports OCABR has received resulted from employee error or other internal mishandling of documents containing personal information. This statistic emphasizes the need to develop, implement, and enforce a CISP with internal data management protocols.

A copy of the finalized regulations, 201 CMR 17.00 et seq., is attached. Additional information about the regulations is available via the OCABR website. Please consult the articles available via our website at http://www.kb-law.com/news/index.php for additional information about Chapters 93H and 93I. Pursuant to the regulations, all businesses must be in compliance by January 1, 2009. Moreover, pursuant to Executive Order 504 signed by Governor Patrick on September 19, 2008, on or after the January 1 effective date , state agencies may not contract with any business that is not in compliance with these regulations.

We are available to assist you with respect to compliance with these new regulatory requirements. Please contact Attorney Becca Rausch with any questions.

201 CMR 17.00: Standards for The Protection of Personal Information of Residents of the Commonwealth

Section:
17.01: Purpose and Scope
17.02: Definitions
17.03: Duty to Protect and Standards for Protecting Personal Information
17.04: Computer System Security Requirements

17.01 Purpose and Scope

(a) Purpose
This regulation implements the provisions of M.G.L. c. 93H relative to the standards to be met by persons who own,
license, store or maintain personal information about a resident of the Commonwealth of Massachusetts. This
regulation establishes minimum standards to be met in connection with the safeguarding of personal information
contained in both paper and electronic records. Further purposes are to (i) ensure the security and confidentiality of
such information in a manner consistent with industry standards, (ii) protect against anticipated threats or hazards to
the security or integrity of such information, and (iii) protect against unauthorized access to or use of such information
in a manner that creates a substantial risk of identity theft or fraud against such residents.
(b) Scope
The provisions of this regulation apply to all persons that own, license, store or maintain personal information about a
resident of the Commonwealth.

17.02: **Definitions**

The following words as used herein shall, unless the context requires otherwise, have the following meanings:
"Breach of security", the unauthorized acquisition or unauthorized use of unencrypted data or, encrypted electronic
data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of
personal information, maintained by a person or agency that creates a substantial risk of identity theft or fraud against
a resident of the commonwealth. A good faith but unauthorized acquisition of personal information by a person or
agency, or employee or agent thereof, for the lawful purposes of such person or agency, is not a breach of security
unless the personal information is used in an unauthorized manner or subject to further unauthorized disclosure.
“Electronic,” relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic or similar
capabilities.
"Encrypted," the transformation of data through the use of an algorithmic process, or an alternative method at least as
secure, into a form in which meaning cannot be assigned without the use of a confidential process or key, unless
further defined by regulation by the office of consumer affairs and business regulation.

“Person,” a natural person, corporation, association, partnership or other legal entity, other than an agency, executive
office, department, board, commission, bureau, division or authority of the Commonwealth, or any of its branches, or
any political subdivision thereof.
"Personal information," a Massachusetts 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.
“Record” or “Records,” any material upon which written, drawn, spoken, visual, or electromagnetic information or
images are recorded or preserved, regardless of physical form or characteristics.

17.03: **Duty to Protect and Standards for Protecting Personal Information**

Every person that owns, licenses, stores or maintains personal information about a resident of the Commonwealth
shall develop, implement, maintain and monitor a comprehensive, written information security program applicable to
any records containing such personal information. Such comprehensive information security program shall be
reasonably consistent with industry standards, and shall contain administrative, technical, and physical safeguards to
ensure the security and confidentiality of such records. Moreover, the 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, licenses, stores or maintains such information may be
regulated.
Whether the comprehensive information security program is in compliance with these regulations for the protection of
personal information, whether pursuant to section 17.03 or 17.04 hereof, shall be evaluated taking into account (i) the
size, scope and type of business of the person obligated to safeguard the personal information under such
comprehensive information security program, (ii) the amount of resources available to such person, (iii) the amount of
stored data, and (iv) the need for security and confidentiality of both consumer and employee information. Without
limiting the generality of the foregoing, every comprehensive information security program shall include, but shall not
be limited to:
(a) Designating one or more employees to maintain the comprehensive information security program;
(b) Identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality,
and/or integrity of any electronic, paper or other records containing personal information, and evaluating and

improving, where necessary, the effectiveness of the current safeguards for limiting such risks, including but not
limited to: (i) ongoing employee (including temporary and contract employee) training; (ii) employee compliance with
policies and procedures; and (iii) means for detecting and preventing security system failures.
(c) Developing security policies for employees that take into account whether and how employees should be
allowed to keep, access and transport records containing personal information outside of business premises.
(d) Imposing disciplinary measures for violations of the comprehensive information security program rules.
(e) Preventing terminated employees from accessing records containing personal information by immediately
terminating their physical and electronic access to such records, including deactivating their passwords and user
names.
(f) Taking reasonable steps to verify that third-party service providers with access to personal information have
the capacity to protect such personal information, including (i) selecting and retaining service providers that are
capable of maintaining safeguards for personal information; and (ii) contractually requiring service providers to
maintain such safeguards. Prior to permitting third-party service providers access to personal information, the person
permitting such access shall obtain from the third-party service provider a written certification that such service
provider has a written, comprehensive information security program that is in compliance with the provisions of these
regulations.
(g) Limiting the amount of personal information collected to that reasonably necessary to accomplish the
legitimate purpose for which it is collected; limiting the time such information is retained to that reasonably necessary
to accomplish such purpose; and limiting access to those persons who are reasonably required to know such
information in order to accomplish such purpose or to comply with state or federal record retention requirements.
(h) Identifying paper, electronic and other records, computing systems, and storage media, including laptops and
portable devices used to store personal information, to determine which records contain personal information, except
where the comprehensive information security program provides for the handling of all records as if they all contained
personal information.
(i) Reasonable restrictions upon physical access to records containing personal information, including a written
procedure that sets forth the manner in which physical access to such records is restricted; and storage of such
records and data in locked facilities, storage areas or containers.
(j) Regular monitoring to ensure that the comprehensive information security program is operating in a manner
reasonably calculated to prevent unauthorized access to or unauthorized use of personal information; and upgrading
information safeguards as necessary to limit risks.
(k) Reviewing the scope of the security measures at least annually or whenever there is a material change in
business practices that may reasonably implicate the security or integrity of records containing personal information.

(l) Documenting responsive actions taken in connection with any incident involving a breach of security, and
mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to
protection of personal information.

17.04: **Computer System Security Requirements**

Every person that owns, licenses, stores or maintains personal information about a resident of the Commonwealth
and electronically stores or transmits such information shall include in its written, comprehensive information security
program the establishment and maintenance of a security system covering its computers, including any wireless
system, that, at a minimum, shall have the following elements:
(1) Secure user authentication protocols including:
(i) control of user IDs and other identifiers;
(ii) a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies,
such as biometrics or token devices;
(iii) control of data security passwords to ensure that such passwords are kept in a location and/or format that
does not compromise the security of the data they protect;
(iv) restricting access to active users and active user accounts only; and
(v) blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation
placed on access for the particular system;
(2) Secure access control measures that:
(i) restrict access to records and files containing personal information to those who need such information to
perform their job duties; and
(ii) assign unique identifications plus passwords, which are not vendor supplied default passwords, to each
person with computer access, that are reasonably designed to maintain the integrity of the security of the access
controls;
(3) To the extent technically feasible, encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data to be transmitted wirelessly.
(4) Reasonable monitoring of systems, for unauthorized use of or access to personal information;
(5) Encryption of all personal information stored on laptops or other portable devices;
(6) For files containing personal information on a system that is connected to the Internet, there must be reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the
integrity of the personal information.
(7) Reasonably up-to-date versions of system security agent software which must include malware protection
and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with
up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis.
(8) Education and training of employees on the proper use of the computer security system and the importance
of personal information security.

17.05: **Effective Date**

These regulations shall take effect on January 1, 2009.
REGULATORY AUTHORITY:
201 CMR 17.00: M.G.L. c. 93H