KROKIDAS & BLUESTEIN
ATTORNEYS
600 ATLANTIC AVENUE
BOSTON, MASSACHUSETTS 02210
PHONE 617-482-7211 • FAX 617-482-7212

CLIENT ALERT

NEW MASSACHUSETTS LAW IMPOSES RECORDS REQUIREMENTS FOR ALL ORGANIZATIONS, INCLUDING THOSE NOT SUBJECT TO HIPAA

Governor Patrick recently signed into effect a law concerning security breach notifications and document destruction requirements that pertains to any organization with access to records containing personal information about Massachusetts residents, regardless of whether the organization is a covered entity under the Health Information Portability and Accountability Act of 1996 ("HIPAA"). A copy of the new law is attached. The Office of Consumer Affairs and Business Regulation ("Consumer Affairs") is charged with promulgating regulations interpreting and implementing the new law. We will continue to monitor developments in this area. In addition, we are available to assist you in complying with federal and state law in connection with the management of security breaches and in developing and implementing security and documentation retention policies.

I. Chapter 93H: Security Breach Notification Requirements

Effective October 31, 2007, the new Chapter 93H of the Massachusetts General Laws will require all organizations with access to confidential personal information about Massachusetts residents to make prompt reports in the case of inadvertent disclosure of that personal information. Specifically, for any organization that owns or licenses personal information about Massachusetts residents, if there is actual knowledge or reason to suspect an unauthorized release, use, or acquisition of such information, three notices of the security breach must be provided promptly: (1) the Office of the Attorney General ("AG"); (2) the Director of Consumer Affairs; and (3) the affected individual. Organizations that only maintain or store such personal data, rather than having direct ownership of or licensure to it, must only provide notice to the data owner/licensee. The owner/licensee must then make the three above required notifications.

Organizations that fail to comply with Chapter 93H will now be subject to suit by the AG under Chapter 93A, the Consumer Protection Law. Violations of the law may give rise to triple damages, as well as liability for attorney's fees and costs in such a suit brought by the AG.

For organizations already subject to HIPAA, Chapter 93H imposes additional considerations. First, Chapter 93H's notice requirements go beyond the more general HIPAA duty to mitigate the effects of an inadvertent disclosure. Second, as noted above, Chapter 93H creates the new state cause of action under Chapter 93A for failing to follow security breach procedures. Third, it will be important to determine how the 93H regulations intersect with

HIPAA, particularly with respect to requirements relating to protecting data to prevent security breaches. Fourth, with these considerations in mind, it may be prudent to incorporate a reference to Chapter 93H in all new Massachusetts business associate agreements to put both parties on notice of the new Massachusetts legal requirements that supplement HIPAA – it is a logical placeholder.

The good news for HIPAA covered entities is that with respect to compliance, Chapter 93H states that if your organization's existing security breach policies and procedures are in good shape and fully comply with federal laws, your organization will be deemed to comply with Chapter 93H – provided that the three new notification requirements are met. The new requirements should be added to your existing policies.

For organizations NOT subject to HIPAA, you must comply with Chapter 93H. If you do not yet have policies in place that address security breaches, such policies need to be prepared and implemented immediately. Regulations to be promulgated pursuant to the new law may provide guidance on the particular provisions to include in the policies.

II. Chapter 93I: Document Destruction Requirements

The new Chapter 93I of the Massachusetts General Laws takes effect on February 3, 2008. Chapter 93I requires all organizations that dispose of records containing personal information about Massachusetts residents to destroy such records, whether paper or electronic, "so that personal information cannot practicably be read or reconstructed." The law does not provide any guidance as to how organizations should comply with this requirement. Organizations may contract with third parties such as data management companies to appropriately destroy records, provided that the third party implements and monitors compliance with Chapter 93H and HIPAA (as applicable) to ensure against unauthorized use, access to, or acquisition of the records.

Any organization that violates the destruction requirements faces a civil fine of up to $100 per person affected by the violation, with a total possible fine of $50,000 for each instance of improper disposal. In addition, as described above, the AG may file suit pursuant to Chapter 93A for failure to comply with Chapter 93I.