KROKIDAS & BLUESTEIN

ATTORNEYS

CLIENT ALERT

RECENT HIPAA AND STATE PRIVACY DEVELOPMENTS

Several Massachusetts healthcare providers have received unwanted press recently due to patients' medical information becoming compromised. These incidents suggest that individuals have greater incentives than ever to enforce their privacy rights against healthcare providers. In view of these events and other recent regulatory changes, healthcare providers need to consider taking additional precautions both to ensure that their patients' privacy is protected and to protect themselves in the event of a claim. This Client Alert summarizes these recent developments and makes recommendations regarding policies and procedures to assure compliance and minimize exposure.

Ruling Lowers Bar For Bringing a Claim Under Massachusetts Right of Privacy Statute:

In May of this year, the Massachusetts Superior Court issued a ruling that may make it easier for individuals whose personal information has been improperly disclosed to claim that their privacy rights have been breached. In Alexander v. Clarke, 28 Mass. L. Rptr. 291 (May 30, 2011), Alexander, a prison inmate, sued her healthcare provider and others after she learned that the provider sent medical information about her to another inmate in a lawsuit to which Alexander was not a party. The medical information at issue related to Alexander's hair loss. Alexander sued under a number of privacy rights statutes, including G.L c. 214, §1B, which authorizes money damages against private individuals and entities.

Notably, the Court held that the improper disclosure of personal information need not be on-going or malicious, and can in fact result from an unintentional action where minimal personal information is disclosed. In Alexander's case, the judge found that hair loss is a personal and sensitive topic, and its disclosure constitutes the type of private and intimate information that would give rise to a valid breach of privacy claim under G.L. c.214, §1B. Therefore, while an individual must still prove damages from a breach of his or her privacy rights, this decision potentially lowers the bar for filing a lawsuit.

HITECH Act Provides Incentives to Report Breaches:

Under federal law, recent regulatory changes place additional responsibilities on healthcare providers regarding patient privacy. The Health Information Technology for

Economy and Clinical Health Act of 2009 (HITECH Act) increased individuals' rights under HIPAA. Individuals whose protected health information has been improperly disclosed under HIPAA are now eligible to receive a percentage of any civil monetary penalties recovered by the government. While HIPAA does not create a private cause of action for individuals, the new right under the HITECH Act gives them a greater incentive to report breaches.

OCR Releases HIPAA Compliance Hotspots:

The Office of Civil Rights, the federal agency which enforces HIPAA, recently released the following compliance hotspots, which are top areas of interest on its HIPAA radar:

- Incident detection and response
- Review of log access
- Secure wireless networks
- Management of user access and passwords
- Theft or loss of mobile devices
- Up-to date software
- Role based access - lack of information access management

Protecting Your Organization:

Now is a good time to revisit your organization's privacy policies and procedures regarding personal information to ensure compliance with the relevant data privacy regulations.

Compliance steps include:

- Encrypting electronic protected health information. This will create the equivalent of a safe harbor from potential HIPAA violations.

  See
  http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/hitechrfi.pdf

- Implementing a Written Information Security Plan (WISP) that is required by the Massachusetts data security laws, G.L. c. 93H and 201 CMR 17.03, which will:

  - Ensure the security and confidentiality of personal information;
  - Protect against any anticipated threats to the security or integrity of such information; and
  - Protect against unauthorized access to or use of such information in a manner that creates a substantial risk of identity theft or fraud.

- Reviewing your business associate agreements. Under the HITECH Act, the HIPAA security and privacy regulations now apply to a business associate of a covered entity in the same manner as the regulations apply to the covered entity.

- Reviewing your insurance policies to confirm that they cover breaches of personal information. Complying with applicable reporting in the event of a data breach

can be time consuming and costly, and insurance policies vary in their coverage for these costs. You should not assume that your policies cover breaches of personal information and should do a careful review of your comprehensive general liability insurance and other policies with your insurance broker, and, if necessary, your legal counsel to assure adequate protection.

For further information on implementing privacy policies and procedures contact Attorney Emily Kretchmer (ekretchmer@kb-law.com), Attorney Jennifer Gallop (jgallop@kb-law.com) or Attorney Anjali Waikar (awaikar@kb-law.com).