HUNTON& WILLIAMS

CLIENT ALERT

May 2009

Contacts

Lisa J. Sotto
200 Park Avenue
New York, NY 10166
(212) 309-1223
lsotto@hunton.com

Elizabeth H. Johnson
One Bank of America Plaza, Suite 1400
421 Fayetteville Street
Raleigh, NC 27601
(919) 899-3073
ehjohnson@hunton.com

Melinda L. McLellan
200 Park Avenue
New York, NY 10166
(212) 309-1163
mmclellan@hunton.com

Additional Lawyers
Cédric Burton
Purdey Castle
Jörg Hladjk
Natalie Hunt
Christopher Kuner
Ryan P. Logan
Manuel E. Maisog
Olivier Proust
Boris Segalis
Aaron P. Simpson
Rachel M. St. John
Bridget C. Treacy
Mason A. Weisz
John W. Woods, Jr.

Centre for Information Policy Leadership
Martin E. Abrams*
Paula J. Bruening
Fred H. Cate
Orson Swindle*

*Not a lawyer

First Enforcement of New California Medical Privacy Provisions: $250,000 Fine Imposed

On May 14, 2009, the California Department of Public Health issued an Administrative Penalty Notice to the Kaiser Foundation Hospital — Bellflower for patient medical information privacy violations. Although the state did not identify the affected patient by name, the facts and circumstances described in the Notice correspond to the case of Nadya Suleman, the single mother of six who gave birth to octuplets at Bellflower in January 2009. The hospital was fined $250,000 for failure to prevent unlawful or unauthorized access to, or use or disclosure of, a patient's medical information as required by new provisions recently added to California's Health and Safety Code. California law also requires health care providers and facilities to notify the Department of any unlawful or unauthorized access to patient medical information within five days of detecting such access. These provisions were reportedly enacted in the wake of several high-profile health data compromises at California health care facilities involving celebrities such as Farrah Fawcett, Britney Spears and California first lady Maria Shriver.

Since California's new privacy provisions came into effect on January 1, 2009, hospitals have reported approximately 300 incidents of inappropriate or unauthorized disclosure of patient information. The Bellflower facility is the first to be sanctioned. Whereas other reported breaches have tended to be inadvertent or negligent in nature, in this case, the agency found that the violations were deliberate, extended beyond the Bellflower facility, and continued even after Kaiser informed regulators that it had suffered a breach. The penalties applicable to Kaiser exceeded the statutory maximum of $250,000 per reported incident, including a $25,000 fine per patient whose medical information was unlawfully accessed (one, in this case), plus a $17,500 fine for each of the 22 subsequent occurrences of unlawful or unauthorized access to that patient's medical information. Kaiser may appeal the penalty by requesting a hearing within 10 calendar days of notification.

In addition to the monetary penalty, Kaiser was subject to an exit conference with state inspectors who visited the facility to determine compliance with state licensing regulations. Kaiser is required to submit a plan of correction for each deficiency noted, including: (1) how each correction will be accomplished, both temporarily and permanently; (2) the title or position of the person responsible for corrections; (3) a description of the monitoring process that will be implemented to prevent recurrence of deficiencies; and (4) the date the deficiency will be corrected. Kaiser must provide the plan within 15 calendar days of receiving the agency's

statement of deficiencies (issued May 14, 2009), and "immediate correction of the deficiency" is expected to occur no more than 30 days from the date of the exit conference.

The Administrative Penalty Notice is available here.

More information about the relevant provisions of California's medical privacy laws can be found here on Hunton & Williams' Privacy and Information Security Law Blog.

We Can Help

In addition to California's requirement that health care providers notify the Department of Public Health of privacy breaches, the recently-enacted federal stimulus bill, known as the American Recovery and Reinvestment Act, imposes soon-to-be-effective information security breach notification requirements on HIPAA-covered entities, their business associates, vendors of personal health records and other entities when unsecured protected health information is affected by the breach. More than 45 states had earlier enacted breach notification laws relevant to certain types of personal information, which in two states includes health or medical information. In addition to breach notification laws, many states now require businesses that maintain personal information to implement data security measures. Hunton & Williams' Privacy and Information Management practice assists clients in developing, implementing and evaluating privacy and information security programs to comply with applicable federal and state requirements. If you would like assistance in reviewing your organization's privacy or data security practices, or developing new policies or training programs, please contact us.

Visit the Privacy and Information Security Law Blog at www.huntonprivacyblog.com for global privacy and information security law updates and analysis.