Document hosted at JDSUPRA
http://www.jdsupra.com/post/documentViewer.aspx?fid=acd96d6a-b1cc-4109-8acf-ae703974f468

Client Advisory - Final Rules Issued for Breach of Electronic Health Information

September 2009
Eric D. Fader

In the last week of August, the Department of Health and Human Services ("HHS") and the Federal Trade Commission ("FTC") officially published their final rules concerning consumer notification of breaches of protected health information ("PHI"). Congress mandated that both rules be issued under the Health Information Technology for Economic and Clinical Health ("HITECH") Act, part of the American Recovery and Reinvestment Act of 2009.

The HITECH Act expanded the reach of the health data breach notification rules to personal health record (PHR) vendors and entities that market devices that allow consumers to upload their own health information. Some examples of these types of devices are body composition analyzers, blood pressure cuffs and pedometers. This marks the first time that federal medical privacy regulations have been applied to organizations that are not "covered entities" or their business associates, and also marks the first time that HHS and the FTC have been directed by Congress to engage in coordinated rulemaking.

The new HHS rule applies to HIPAA-covered entities and their business associates, while the new FTC rule applies to PHR vendors and related entities, and third-party service providers to such entities. The FTC and HHS intend to work together in enforcing the rules. Both rules require that consumers affected by a breach involving unsecured PHI be notified in writing within 60 days following the discovery of the breach, and business associates and service providers to one of these entities must promptly notify the entity of a breach so that it may notify consumers. The FTC rule also formally adopts HHS guidance on methodologies and technologies to render PHI "secured" (unusable, unreadable, or indecipherable to unauthorized parties). The rules specify the method and content of breach notification, both to consumers and to HHS and the FTC, as applicable. An entity whose breach affects 500 or more people must also notify local media outlets.

The new rules will apply to both intentional and unintentional breaches of PHI, ranging from a nurse accidentally faxing a patient's medical test report to the wrong telephone number to a rogue employee improperly selling patients' prescription information to a pharmaceutical marketing company. There is little doubt that the FTC and HHS will be kept quite busy processing breach notifications; by way of example, the California Department of Public Health received more than 800 reports of health data breaches in the first five months after a new state law became effective on January 1, 2009.

The HHS and FTC rules will become effective 30 days after their publication in the Federal Register, or September 24 and 25, respectively. However, both agencies stated that they will use their enforcement discretion to refrain from bringing an enforcement action for failure to provide the required notifications for breaches that are discovered within 180 days after publication of the rules. Also, HHS is seeking comments on the provisions of its rule (which is technically an "interim final rule ") within 60 days after its publication.

Document hosted at JDSUPRA
http://www.jdsupra.com/post/documentViewer.aspx?fid=acd96d6a-b1cc-4109-8acf-ae703974f468

As the above is but a brief summary of two very complex rules, interested parties should review the rules in detail and contact one of the members of our Privacy Group with any questions.

HHS news release:

http://www.hhs.gov/news/press/2009pres/08/20090819f.html

FTC news release:

http://www.ftc.gov/opa/2009/08/hbn.shtm

This advisory is for guidance only and is not intended to be a substitute for specific legal advice. If you would like further information, please contact the Edwards Angell Palmer & Dodge LLP attorney responsible for your matters or one of the attorneys listed below:

Eric D. Fader, Counsel	212.912.2724	efader@eapdlaw.com
Mark E. Schreiber, Partner and Chair, Privacy Group	617.239.0585	mschreiber@eapdlaw.com
Theodore P. Augustinos, Partner	860.541.7710	taugustinos@eapdlaw.com
Laurie Kamaiko, Partner	212.912.2768	lkamaiko@eapdlaw.com
Richard Hopley, Partner	+44.207.556.4532	rhopley@eapdlaw.com
Pat Concannon, Counsel	617.239.0419	pconcannon@eapdlaw.com
Joseph Geoghegan, Associate	860.541.7749	jgeoghegan@eapdlaw.com
Socheth Sor, Associate	860.541.7773	ssor@eapdlaw.com
Sam Tacey, Solicitor	+44.207.556.4528	stacey@eapdlaw.com