porterwright

Information Privacy & Data Security and Health Care Law Alert

A Corporate Department Publication

August 21, 2009

This Information Privacy & Data Security and Health Care Law Alert is intended to provide general information for clients or interested individuals and should not be relied upon as legal advice. Please consult an attorney for specific advice regarding your particular situation.

Donna M. Ruscitti
614-227-2192
druscitti@porterwright.com

Richard G. Terapak
614-227-4301
rterapak@porterwright.com

Kenneth K. Rathburn
614-227-2128
krathburn@porterwright.com

Jeremy A. Logsdon
614-227-2093
jlogsdon@porterwright.com

Robert J. Morgan
614-227-2186
rmorgan@porterwright.com

James H. Prior
614-227-2008
jprior@porterwright.com

Robert W. McAdams, Jr.
614-227-2091
rmcadams@porterwright.com

Timothy B. Mitchell
614-227-2102
tmitchell@porterwright.com

Theodore G. Fisher
614-227-2040
tfisher@porterwright.com

Brian D. Hall
614-227-2287
bhall@porterwright.com

Mark K. Velasco
937-449-6723
mvelasco@porterwright.com

Government Agencies Issue HITECH Act Regulations

This week, two federal agencies have released regulations requiring notification to individuals in the event of a security breach of unsecured protected health information (PHI). Both agencies are acting under the requirements of The American Recovery and Reinvestment Act of 2009 (ARRA), signed into law February 17, 2009, which included what is known as the Health Information Technology for Economic and Clinical Health Act (HITECH Act).

The Department of Health and Human Services (HHS) issued new regulations August 19, 2009 that apply to health care providers, health plans, business associates, and other entities regulated by the Health Insurance Portability and Accountability Act (HIPAA). The regulations will be published in the Federal Register August 24, 2009 and will be effective September 23, 2009. The HHS regulations provide guidance to covered entities and business associates regarding the HITECH Act's new data breach notification requirements. The HITECH Act includes penalties up to $50,000 per violation and up to $1.5 million in a calendar year for a covered entity's failure to notify individuals in accordance with the statute's provisions. For more information and analysis regarding the HITECH Act's specific requirements, see our March 2009 alert ***"HITECH Act Brings New Vigor to HIPAA'sPrivacy and Security Rules."***

The HHS regulations specify the techniques and technologies that such entities can implement that render protected health information unusable, unreadable, or indecipherable to unauthorized individuals. Additionally, the HHS regulations provide a "safe harbor" procedure for covered entities and business associates to follow in order to ensure that any PHI accessed, used, disclosed, or acquired by unauthorized individuals is deemed secured, and in turn relieves the covered entity from its obligation to notify the individuals under HITECH. The HHS regulations also provide additional explanation regarding specific encryption techniques and standards, including specific National Institute of Standards and Technology (NIST) publications regarding encryption technologies, in which HHS has determined that, if followed, renders PHI unusable, unreadable, or indecipherable. Finally, the HHS regulations provide additional commentary and guidance regarding (i) what events or circumstances constitute or may constitute a breach, thereby triggering the

porterwright

HITECH notification requirements; (ii) the interplay between a breach of the HIPAA Privacy Rule and the data breach notification obligations; and (iii) other requirements such as mandatory media outlet notification and required notification of HHS related to breaches affecting more than 500 individuals.

Alternatively, on August 17, 2009 the Federal Trade Commission (FTC) issued a final rule requiring certain non-HIPAA entities, such as vendors of personal health records, to notify consumers when the security of their unsecured personal health records are compromised. The FTC rule applies to entities that are not regulated by HIPAA; however, the breach notification requirements introduced in the HITECH Act place substantially similar notification requirements (including the timing, method, and content requirements of such notice) upon such non-HIPAA entities. The FTC rule is effective 30 days after the date of publication in the Federal Register, and full compliance is required 180 days after the date of publication in the Federal Register. (As of this writing, the publication date is unknown, but will likely be within the next two weeks.)

Both sets of regulations promulgated under HITECH provide clarification and guidance for implementing the law, which significantly increase not only responsibilities of entities dealing with protected health information, but the penalties for non-compliance. Entities covered under these regulations must review current practices and procedures immediately and seek assistance where necessary to achieve compliance with the requirements of these regulations.

Please see our other publications at www.porterwright.com/publications.

Porter Wright Morris & Arthur LLP
www.porterwright.com

Cincinnati, Ohio
800-582-5813
Cleveland, Ohio
800-824-1980
Columbus, Ohio
800-533-2794
Dayton, Ohio
800-533-4434
Naples, Florida
800-876-7962
Washington, DC
800-456-7962