

PUTNEY, TWOMBLY, HALL & HIRSON LLP

DANIEL F. MURPHY, JR.
MICHAEL T. McGRATH
THOMAS A. MARTIN
WILLIAM M. POLLAK
JAMES E. McGRATH, III
CHRISTOPHER M. HOULIHAN
THOMAS M. LAMBERTI
STEPHEN J. MACRI
HARVEY I. SCHNEIDER
MARY ELLEN DONNELLY
JOSEPH B. CARTAFALSA
GEOFFREY H. WARD
ANDREA HYDE
E. PARKER NEAVE
MARK A. HERNANDEZ
JAMES M. STRAUSS
PHILIP H. KALBAN
SEAN H. CLOSE
LANSING R. PALMER
JEROME P. COLEMAN
BARBARA M. MAISTO

ESTABLISHED 1866
COUNSELORS AT LAW
521 FIFTH AVENUE
NEW YORK, NEW YORK 10175
(212) 682-0020
TELEFAX: (212) 682-9380
PUTNEYLAW.COM

120 WOOD AVENUE SOUTH
SUITE 600
ISELIN, NEW JERSEY 08830
(732) 632-2505
TELEFAX: (732) 632-2506
1205 FRANKLIN AVENUE
GARDEN CITY, NY 11530
(516) 746-0070
TELEFAX: (516) 746-0599
2500 NORTH MILITARY TRAIL
SUITE 200
BOCA RATON, FLORIDA 33431
(800) 935-8480
TELEFAX: (561) 393-9707
COUNSEL
CHARLES J. GROPPE
ALEXANDER NEAVE
DUSTAN T. SMITH
SPECIAL COUNSEL
JUDITH M. BANDLER

April 13, 2009

CLIENT ALERT

American Recovery and Reinvestment Act Modifies HIPAA

On February 17, 2009, President Obama signed into law the American Recovery and Reinvestment Act of 2009 (“ARRA” or “the Act”), better known as the federal stimulus package. The ARRA expands the privacy and security provisions of the Health Insurance Portability and Accountability Act (“HIPAA”). Most notably, the Act applies HIPAA provisions and penalties to “business associates,” imposes notice requirements in the case of a HIPAA breach and strengthens enforcement of HIPAA.

“Business Associates” Subject to Rules and Penalties

The Act applies HIPAA penalties and provisions, which were previously applied only to “covered entities,” to “business associates.” “Business associates” are individuals, other than employees of the covered entity, and entities who provide certain services and support to covered entities, and as such would include, for example, data processors, consultants, etc. Covered entities and business associates will have to incorporate this change into their business associate agreements beginning February 17, 2010.

Notice Requirements in Case of Breach

If “unsecured protected health information” has been breached, covered entities must notify within sixty days each individual whose information has been, or is reasonably believed to have been, accessed, acquired, or disclosed as a result of such breach. The Act defines “Unsecured protected health information” as information that is not protected with technologies and methodologies endorsed by the Secretary of Health and Human Services (“the Secretary”). Further information on such technologies can be found at <http://www.hhs.gov/healthit/privacy/hipaa.html> (Note: the Secretary is expected

to update the website with new information). Additionally, if the covered entity believes that the breach compromises the information of more than 500 individuals, the entity must notify prominent media outlets and the Secretary. The notice must include the following:

- (1) A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.
- (2) A description of the types of unsecured protective health information that were involved in the breach (such as full name, Social Security number, date of birth, home address, account number, or disability code).
- (3) The steps individuals should take to protect themselves from potential harm resulting from the breach.
- (4) A brief description of what the covered entity is doing to investigate the breach, to mitigate losses, and to protect against further breaches.
- (5) Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, and e-mail address, Web site, or postal address.

If a business associate discovers a breach, it must notify the covered entity. The notice requirements will take effect thirty days after the Secretary promulgates regulations to carry out the provisions. To date, the Secretary has not announced when said regulations will be promulgated.

Enhanced Enforcement

The Act sets out a tiered increase of civil monetary penalties for violations:

- *First Tier.* If a person did not know (and by exercising reasonable diligence would not have known) that he or she violated a requirement, such person shall incur a penalty of at least \$100 for each violation not to exceed \$25,000 for all violations of the same requirement during a calendar year.
- *Second Tier.* If the violation was due to reasonable cause, the person shall incur a penalty of at least \$1,000 for each violation not to exceed \$100,000 for all violations of the same requirement during a calendar year.
- *Third Tier.* If the violation was due to willful neglect but it was corrected, the person shall incur a penalty of at least \$10,000 for each violation not to exceed \$250,000 for all violations of the same requirement during a calendar year.
- *Fourth Tier.* If the violation was due to willful neglect but it was not corrected, the person shall incur a penalty of at least \$50,000 for each violation not to exceed \$1,500,000 for all violations of the same requirement during a calendar year.

In determining the amount of a penalty, the Secretary shall base such determination on the nature and extent of the violation and the nature and extent of the harm resulting from such violation. Additionally, the Act allows state attorney generals to bring actions to enforce HIPAA on behalf of state residents. These enforcement provisions take effect immediately.

* * * *

The ARRA makes several other changes to HIPAA that may affect your workplace. If you have any questions regarding the new HIPAA provisions, please contact us.

PUTNEY, TWOMBLY, HALL & HIRSON LLP