TUCKER ELLIS & WEST LLP
ATTORNEYS AT LAW

CLIENT ALERT **FEBRUARY 2009**

HEALTH CARE LAW: HIPAA PRIVACY AND SECURITY RULES
STIMULUS LEGISLATION MODIFIES HIPAA RULES FOR PROTECTION OF PHI

BY BERNIE SMITH

On February 17, 2009, President Obama signed into law the "The American Recovery and Reinvestment Act of 2009" (the "Act"), commonly referred to as the "stimulus bill." Most reports on this massive piece of legislation focus on its myriad of grant authorizations and sweeping changes to the tax laws. But make no mistake; the Act affects virtually every department and many regulatory functions of the Federal government. Included among its hundreds of pages are changes to the existing HIPAA rules governing the privacy and security of protected health information ("PHI"). These modifications appear driven, in large part, by the Act's support for the development of nationwide standards for and operability of electronic health records. Many of the new requirements will be of particular concern to business associates and might result in covered entities seeing increases in the cost of doing business with certain parties. At a minimum, covered entities will need to alter some practices and update existing business associate agreements.

NOTIFICATION OF PRIVACY OR SECURITY BREACHES

The Act requires that under certain circumstances, either a covered entity or a business associate give notice to individuals of instances of a "breach" as to what the Act calls "unsecured protected health information." Unsecured protected health information means PHI that is not protected by new security standards designed to render PHI unusable, unreadable or indecipherable to unauthorized individuals. These new standards are to be issued within 60 days after the Act becomes effective. They may include new protective standards adopted in connection with the development and adoption of electronic health records. A "breach" is an unauthorized acquisition, access, use or disclosure of unsecured PHI. Certain inadvertent or unintentional acts are excluded from these new rules.

The Act requires delivery of notice by first class mail to each individual who is or might reasonably have been affected by a breach of unsecured PHI. Under certain scenarios, if notice by mail is not possible, other forms of notice, such as a website posting may be required. If more than 500 residents of a particular state are affected by a breach, notice through public media outlets is required. Notice must also be provided on an occurrence basis or at least annually to the Secretary of Health and Human Services. The Secretary must make information so received available publicly on the HHS website.

NEW REQUIREMENTS FOR BUSINESS ASSOCIATES

The Act imposes on business associates certain security and privacy requirements that under current law apply only to covered entities. These include the obligations to:

- implement administrative, physical and technical safeguards to protect the security of electronic PHI;
- adopt certain security policies and procedures; and

- comply with certain requirements of the privacy rules as if the business associate was itself a covered entity.

These new mandates should be reflected appropriately in a covered entity's standard form of business associate agreement.

The Act also subjects business associates to the same civil and criminal penalties that apply to covered entities in cases where a business associate violates certain of the Act's new rules.

MANDATORY DISCLOSURE RESTRICTIONS

The Act requires that a covered entity honor requests from individuals for restrictions on disclosure of information to health plans for health care operations and payment purposes if the PHI at issue pertains solely to a health care service or item for which the service provider "has been paid out of pocket in full." This is a significant modification to current law which allows a covered entity the discretion to accept or reject an individual's request for restrictions on the disclosure of PHI. It presumably is meant to allow individuals who absorb the full cost of certain medical expenses to keep that information from being shared with health plans. It remains to be seen how this might affect health plans' clinical programs and underwriting.

OTHER CHANGES

There are numerous other changes in the almost fifty pages of the Act dealing with health information. These include:

- additional restrictions on the sale of PHI and its use for fundraising and marketing purposes;
- clarification of rules as to what constitutes a "minimum necessary" amount of PHI;
- treating certain organizations that provide data transmission to a covered entity in connection with electronic health records as a business associate of the covered entity and requiring that the service provider and covered entity enter into a business associate agreement; and
- provisions for improved enforcement of civil and criminal penalties for violations of HIPAA.

The above are just the highlights of the numerous provisions of the Act affecting HIPAA and the privacy and security of PHI. Covered entities are urged to familiarize themselves immediately with the Act's requirements and review their business associate and other relationships to determine how they and related agreements might be affected.

For more information, please contact Bernie Smith by phone at 216-696-3952 or by e-mail at bsmith@tuckerellis.com

****

1150 Huntington Building
925 Euclid Avenue
Cleveland, OH 44115
www.tuckerellis.com