

# **RISK MANAGEMENT Advisory**

## **Changes to HIPAA under the HITECH Act**

The American Recovery and Reinvestment Act of 2009 contains a provision entitled *Health Information Technology for Economic and Clinical Health Act* (HITECH Act). This Act provides funding for health information and technology and includes changes to the Health Insurance Portability and Accountability Act (HIPAA).

Under the HITECH Act, the current HIPAA regulations remain and are expanded in some areas. The following is a brief summary of the changes that will affect health care providers. MMIC will provide additional information on these HIPAA changes in the coming months.

### **Business Associates**

Under the HITECH Act, Business Associates (BA), like Covered Entities (CE), are directly subject to the HIPAA rules, and to civil and criminal penalties and enforcement proceedings.

### **Requirements for notification of a breach**

Covered Entities and BAs have a notification duty if there is a breach of “unsecured protected health information” (PHI), which will be defined by the Secretary of the Department of Health and Human Services (HHS) by April 18, 2009.

A CE must notify the individual, and a BA must notify the CE of a breach no later than 60 days after discovering the breach. The BA must provide the identity of the individual whose unsecured PHI was inappropriately disclosed, accessed or acquired by the breach. The Act provides guidance on how to contact the subject of the breach. The content of 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 if known.
2. A description of the types of unsecured PHI (social security numbers, date of birth, home address) that were involved in the breach.
3. Steps the individual can take to protect themselves from potential harm resulting from the breach.
4. A description of what the CE is doing to investigate the breach, to mitigate losses and to protect against additional breaches.
5. Contact information so individuals can ask questions or get additional information including a toll-free telephone number, an e-mail address, Web site or postal address.

When the breach of unsecured PHI involves more than 500 individuals, the CE must provide notice via a prominent media outlet and notify HHS. Breaches involving fewer than 500 individuals must be reported to the Secretary of HHS annually and may be in a log format. The Secretary of HHS will issue interim final regulations on breach notification requirements no later than August 17, 2009 and will apply to any breach discovered 30 days after the publication of the interim final regulations.

### **Limiting use of certain PHI**

Disclosing health information for payment or health care operations (i.e., not for treatment) must be kept to the “minimum necessary.” The Secretary of HHS will issue further guidance within 18 months on what constitutes minimum necessary. Until that time, CEs and BAs must limit these disclosures to the limited data set.

*continued on next page*

## **Expanding Rights for The Subject of the PHI**

Individuals can request that PHI not be disclosed to health plans. Covered entities must comply with the request if the disclosure does not relate to treatment and if the individual has paid out-of-pocket in full.

## **Increased Civil Sanctions and Clarification of Criminal Penalties**

The Act requires HHS to conduct periodic audits on CEs and BAs to ensure compliance and to investigate and impose a penalty for violations due to willful neglect. The Act provides a four-tiered civil penalty structure base and increases the maximum penalty to \$1.5 million a year for violations of the same requirement for each entity. The Act grants state attorneys general the authority to bring civil actions on behalf of state residents adversely affected by a HIPAA violation. The Act extends criminal penalties to employees who wrongfully disclose PHI.

## **Next Steps**

1. Review and compare current HIPAA privacy and security policies and procedures with the new requirements.
2. Analyze state notification requirements and the new requirements under HITECH.
3. Review and update your business associate agreements.
4. Train all staff on the changes to HIPAA.

MMIC will be closely monitoring developments as they occur and will make every effort to keep you informed.

*For more information on funding for health information technology infrastructure and the incentive programs see "What the Stimulus Bill Means to You: The Health Information Technology for Economic and Clinical Health Act (HITECH Act)" in the first quarter 2009 MMIC Technology Solutions Update newsletter. The newsletter is also available on the MMIC Web sit, [www.mmicgroup.com](http://www.mmicgroup.com), look under publications and corporate newsletters.*



[www.mmicgroup.com](http://www.mmicgroup.com)

### **Minneapolis Office**

7650 Edinborough Way, Suite 400  
Minneapolis, Minnesota 55435-5978  
PH. (952) 838-6700 or 1-800-328-5532  
Fax (952) 838-6808

### **West Des Moines Office**

1415 28th Street, Suite 125  
West Des Moines, Iowa 50266-1463  
PH. 1-800-798-9870  
Fax (515) 222-0966

### **Omaha Office**

10330 Regency Parkway Drive, Suite 302  
Omaha, Nebraska 68114-3736  
PH. 1-888-397-3034  
Fax (402) 397-3899