Merrill Law Firm LLC

Old Spring Grove Bank Building
1927 Main Street
Spring Grove, IL 60081
Phone 815.675.2999
Fax 847.239.7923
Website www.Merrill-Law.com
E-mail Rick@Merrill-Law.com

MEMORANDUM

Date: July 14, 2009

From: Richard W. Merrill, Jr.

Re: Summary of HITECH Act of 2009

The Health Information Technology for Economic and Clinical Health Act (HITECH Act) was signed into law on February 17, 2009 as part of the Title XIII of the American Recovery and Reinvestment Act of 2009 (ARRA) and sets forth a federal standard for security breach notifications relating to the unauthorized dissemination of protected health information (PHI). The Health Insurance Portability and Accountability Act of 1996 (HIPAA) does not currently require covered entities to report and/or notify individuals or government agencies of any unauthorized access to and/or dissemination of PHI. Section 13402 of the HITECH Act requires covered entities (as defined by HIPAA) to notify individuals if there has been a breach of their unsecured protected health information (UPHI). Section 13407 of the HITECH Act sets forth breach notification requirements for vendors of personal health records (PHR) and related entities that are not subject to the HIPAA requirements.

Section 13402 of the HITECH Act requires cover entities and business associates in the event of a breach of any PHI to notify each individual who's UPHI has been, or is reasonably believed by the covered entity to have been disclosed without authorization. Unsecured protected health information is defined as PHI that "is not secured through the use of a technology or methodology" specified by the Secretary of the Department of Health and Human Services (DHHS) in guidance that was issued on April 17, 2009. The DHHS guidance sets forth the technologies and methodologies that covered entities should employ to render PHI unusable, unreadable or indecipherable to unauthorized individuals. The term "breach" is defined by the HITECH Act as the "unauthorized acquisition, access, use or disclosure of protected health information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information."

In the event of any breach of any UPHI, the covered entity must notify all affected individuals without reasonable delay but in no case later that sixty (60) calendar days after the discovery of the breach by the covered entity. Written notice may be sent to the individual by first class mail at the last known address or by electronic mail, if specified by the individual. Section 13402 of the HITECH Act also provides for emergency and/or substitute delivery methods for the notice. In the event the breach of UPHI affects more than 500 residents of a State or jurisdiction, the covered entity is require to notify (i) prominent media outlets serving said State or jurisdiction; and (ii) the Secretary of DHHS which will post said breach on the DHHS website.

The content of the breach notice (regardless of the delivery method) must include the following:

(i) A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.
(ii) A description of the types of UPHI that were involved in the breach.
(iii) The steps individuals should take to protect themselves from potential harm resulting from the breach.
(iv) A brief description of what the covered entity involved is doing to investigate the breach, to mitigate losses, and to protect against any further breaches.
(v) Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, website or postal address.

Section 13407 of the HITECH Act requires a vendor of personal health records following the discovery of a breach of security of unsecured PHR identifiable health information to notify: (i) each individual who is a citizen or resident of the United States whose unsecured PHR identifiable health information was acquired by an unauthorized person as a result of such a breach of security; and (ii) the Federal Trade Commission (FTC). In addition, third party service providers that that provide services to a vendor of PHR must notify said vendor following the discovery of a breach security of unsecured PHR identifiable health information to notify said vendor of the breach. The term "PHR identifiable information" is defined as individually identifiable health information (as defined by HIPAA) and includes information "that is provided by or on behalf of the individual; and that identifies the individual or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual." The content of the breach notice and method of delivery is the same as set forth in Section 13402 of the HITECH Act.

The HITECH Act requires the FTC to issue interim rules implementing breach notifications requirements for PHR vendors and certain other non-HIPAA covered entities on or before August 16, 2009. The HITECH Act also requires the DHHS and FTC to submit a joint report to Congress by February 17, 2010 on privacy, security and breach notification requirements for entities that are not HIPAA covered entities or business associates, such as PHR vendors and other related entities and service providers. HIPAA covered entities, business associates, PHR vendors, PHR related entities and third party service vendors will be required to be in compliance with the federal breach notifications provisions within thirty days from the issuance of the interim final regulations.