Data Breach Notification - Part I

Data Breach Notification - Part I

Insight — 7/1/2009

The American Recovery and Reinvestment Act of 2009 ("ARRA") added a data breach notification provision to HIPAA. This provision requires a covered entity that accesses, maintains, retains, modifies, records, stores, destroys or otherwise holds, uses or discloses unsecured protected health information to notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, or disclosed as a result of a breach. This notification requirement applies to all unsecured protected health information whether in electronic, paper or other form.

On April 17, 2009, as required by ARRA, the Secretary of Health and Human Services issued guidance to define what constitutes secured protected health information within the meaning of the American Recovery and Reinvestment Act of 2009. In short, secured protected health information is protected health information that is protected by one of the encryption methodologies specified in the guidance or that is destroyed. This effectively means that health records maintained in paper form are always unsecure for purposes of this data breach notification requirement.

This provision of HIPAA defines "breach" to mean 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.

ARRA then goes on to define exceptions to the definition of breach and provides the following:

1. It is not a breach when there is an unintentional acquisition, access or use of protected health information by an employee or individual acting under the authority of a covered entity or business associate if the acquisition, access or use was made in good faith and within the course and scope of employment or other professional relationship and such information is not further acquired, access, used or disclosed by any person
2. It is not a breach when there is an inadvertent disclosure from an individual who is authorized to access the protected health information at a facility operated by a covered entity or business associate to another similarly situated individual at the same facility. In this circumstance for the disclosure to not be a breach, the information received as a result of the disclosure cannot be further acquired, accessed, used or disclosed without authorization.

This data breach notification requirement places additional obligations on covered entities and can certainly result in increased costs if a covered

entity has to provide notification as required by these new HIPAA provisions. The exceptions provide some relief from the breach notification requirement for the kind of unintentional or inadvertent disclosures that can occur in the work place despite the best efforts of the covered entity.

Subscribe to get our Insights delivered to your inbox.