Data Breach Notification - Part II

Data Breach Notification - Part II

Insight — 7/2/2009

As discussed in the previous article on data breach, the American Recovery and Reinvestment Act of 2009 ("ARRA") added a provision that requires a covered entity to notify each individual whose unsecured protected health information has been or is reasonably believed to have been accessed, acquired or disclosed as a result of a breach. For purposes of ARRA, a breach is discovered by the covered entity or by a business associate as of the first day on which the breach is known to the covered entity or business associate or to any person other than the person committing the breach that is an employee, officer or other agent of the covered entity or business associate. The date of discovery is important because once a breach is discovered, the covered entity must make the required notices no later than 60 days after discovery.

Notice must also be provided to prominent media outlets if the data breach involves unsecured protected health information of more than 500 residents of a state or jurisdiction. Notice must also be provided to the Secretary of Health and Human Services. If the data breach involves the unsecured protected health information of 500 or more individuals, this notice must be provided immediately. If the data breach involves less than 500 individuals, the covered entity may maintain a log of any such breach and submit the log to the Secretary of Health and Human Services annually.

If there is insufficient or out-of-date contact information for 10 or more individuals, the covered entity must post notice on the home page of the covered entity's website or provide notice in major print or broadcast media.

Notice of a breach must include a brief description of what happened, the date of the breach and of discovery of the breach, the types of unsecured protected health information involved in the breach, steps individuals should take to protect themselves, and a brief description of what the covered entity is doing to investigate the breach, mitigate losses and protect against further breaches. Finally, the notice must provide contact information for individuals to ask questions or learn additional information.

As can be seen from the above requirements, the financial cost to a covered entity that suffers a breach of unsecured protected health information can be substantial. Not only must a covered entity incur the cost of notification but it must also fix the problem and mitigate the losses. In addition, this new legislation requires public disclosure of a data breach which may have its own cost in the form of damage to a covered entity's reputation.

Subscribe to get our Insights delivered to your inbox.

This publication is designed to provide general information on pertinent legal topics. The statements made are provided for educational purposes only. They do not constitute legal or financial advice nor do they necessarily reflect the views of Holland & Hart LLP or any of its attorneys other than the author(s). This publication is not intended to create an attorney-client relationship between you and Holland & Hart LLP. Substantive changes in the law subsequent to the date of this publication might affect the analysis or commentary. Similarly, the analysis may differ depending on the jurisdiction or circumstances. If you have specific questions as to the application of the law to your activities, you should seek the advice of your legal counsel.