State Privacy Breach Laws May Trump HIPAA/HITECH

When HITECH amended HIPAA in 2009 it empowered state attorneys general to sue breaching parties to enforce the privacy and security rights of their respective state's citizens. Prior to this time only the Department of Health and Human Services (DHHS) was permitted to enforce HIPAA. However, § 13410(e) of the HITECH Act limits the money damages that attorneys general can collect to $100 per individual affected, however not to exceed $25,000 for all violations of an identical requirement or prohibition during a calendar year.

Some state health privacy laws impose higher money penalties on breaching parties, and recently the Indiana Attorney General invoked state law, over HIPAA/HITECH, when prosecuting a privacy breach by insurer WellPoint, Inc. In that instance, the applicable Indiana statute permitted recovery of up to $150,000 per failure to disclose a health data security breach.

In the WellPoint breach, applications for individual health insurance policies containing Social Security numbers, financial and health information for 32,051 Indiana residents were accidentally made available on the internet for at least 137 days between October 2009 and March 2010. A member of the public notified WellPoint of the problem on February 22, and ultimately the individual filed a class action lawsuit against WellPoint on March 8. After being sued WellPoint quickly fixed the online problem, which had occurred during a system upgrade. However, WellPoint did not begin notifying its customers of the breach until June 18. And, when it did notify customers in Indiana, it did not notify the Attorney General, as required under state law.

WellPoint notified the DHHS of the breach in accordance with HITECH. However when Greg Zoeller, the Indiana Attorney General, filed suit against WellPoint in October 2010, it did so not under HITECH but under a provision of the Indiana Code allowing recovery of up to $150,000 per "deceptive act," which term included a failure to disclose a breach of the security of personal data. The Indiana statute also allows recovery of the Attorney General's reasonable investigation and prosecution costs.

Regarding this choice of law, a spokesperson for the Indiana Attorney General's office stated:

> "While the option to file under HITECH/HIPAA in federal court was considered, Indiana's notification laws and enforcement options allow greater remedies . . . . [u]nder HITECH/HIPAA, the possible penalties maximum would have been $25,000 vs. $300,000 under Indiana law." (Presumably the two "deceptive acts" were delayed notification of the public and failure to notify the Indiana AG).

WellPoint ultimately reached a settlement with the Attorney General on June 23, 2011, pursuant to which it will pay a $100,000 fine to a state fund providing restitution to defrauded consumers and will provide two years of credit monitoring and identity theft protection to affected individuals in Indiana. In addition, it will reimburse victims of identity theft for losses up to $50,000 per individual.

Prior to this case, the Connecticut Attorney General sued Health Net under HITECH/HIPAA following the insurer's delayed notification of its loss of an unencrypted portable disk drive holding records for more than 500,000 insureds in Connecticut and more than 1.5 million nationwide. In that settlement HealthNet agreed to pay $250,000 in damages, provide two years of credit monitoring, $1 million of identity theft insurance and reimburse the costs of security credit freezes.

When HITECH first empowered attorneys general to prosecute data security breaches, little thought was given to the possibility that they might have more leverage under state laws than under the new federal statute. With state budgets stretched to the limit, this may prove more of a factor in which security breaches are prosecuted, and under which laws.

California law permits individuals to sue over breaches of their personal security data and recover up to $3,000 per violation as well as attorneys' fees, but neither mandates the contents of security breach notices, nor requires notification of the California Attorney General. This may change, however, as a California Senate bill would specify the contents of breach notifications and, and for breaches affecting more than 500 California residents would require that breach notifications be sent electronically to the Attorney General. The Senate passed SB 24 in April 2011 and it is easily passing committee votes in the State Assembly. I will continue to update the progress of the bill in future articles.