BCLP. Client Intelligent

**BenefitsBCLP**

# DATA SECURITY BREACHES – ARE YOU PREPARED?

Mar 16, 2012

In the event of a data security breach, evaluating the situation and taking action right away is important. One type of data security breach that employers need to be aware of and that has been receiving attention lately relates to the privacy and security of health information. Over the past year, enforcement of the HIPAA Privacy and Security Rules has become a priority for the Department of Health and Human Services ("HHS") Office of Civil Rights ("OCR"), as seen by the amount of settlement fines related to violations and the recent flurry of HIPAA compliance audits. For example, last year, Massachusetts General Hospital was fined $1 million to settle potential HIPAA violations related to patient information left on a train by an employee commuting to work. Just this week, HHS announced that Blue Cross Blue Shield of Tennessee agreed to pay $1.5 million to settle possible violations of the HIPAA privacy and security rules, which was the first enforcement action which resulted from a breach report required by the Health Information Technology for Economic and Clinical Health ("HITECH") Act Breach Notification Rule.

This increased activity in HIPAA enforcement is the result of provisions in the HITECH Act, which introduced new breach notification standards and requires OCR to develop procedures for auditing compliance with HIPAA.

**HITECH Requirements**

The HITECH Act, enacted in 2009, addresses the privacy and security concerns associated with the electronic transmission of health information, in part, through several provisions that strengthen the civil and criminal enforcement of the HIPAA rules. In the event of a breach of any protected health information ("PHI"), covered entities have an obligation under HIPAA to mitigate, to the extent practicable, any harmful effects that are known to the covered entity as a result of the breach. In addition, under HITECH, if the breach involves "unsecured PHI" (or a reasonable belief of such breach), a covered entity must give certain required notifications of the breach. The required notifications must be made without unreasonable delay and in no case later than 60 calendar days after discovery of the breach (or when the breach would have been discovered had reasonable diligence been exercised).

The covered entity should notify the individual in writing by first-class mail (or e-mail if the individual indicated such preference). The covered entity may also telephone individuals (in

addition to written notification) if the notice is deemed urgent because of possible imminent misuse of unsecured PHI. Notice must also be provided to HHS and, if the breach involves more than 500 individuals, prominent media outlets. The covered entity has the burden of proving that the required notifications were made or that the use or disclosure did not constitute a breach.

**Other Data Security Breach Reporting Requirements**

As benefits professionals we are especially aware of HITECH's requirements but, in the event of any data security breach, employers need to consider whether other statutes apply. For example, since 2004, almost every state has adopted a statute that requires companies to notify consumers and/or employees if their sensitive information may have been obtained by an unauthorized third party. As another example, public companies should consider guidance from the Security and Exchange Commission issued last year regarding the disclosure of cybersecurity incidents in their disclosure statements.

As a convenience for our clients, Bryan Cave has launched a data breach hotline. An attorney from our Data Privacy & Security Team is available 24 hours a day to advise clients on what to do when their data may have been accessed by an unauthorized party, lost, or accidentally disclosed (including a breach of PHI). How our clients respond in the first 24 hours following any type breach has a dramatic effect on our ability to defend them in resulting investigations and litigation. When a security breach occurs, preventing liability often means analyzing the facts, identifying legal obligations, and taking steps to prevent or mitigate harm within the first minutes or hours. The Bryan Cave Data Privacy & Security Team launched the hotline to leverage our depth of knowledge and geographic platform to provide clients with immediate help.

## MEET THE TEAM


### Denise Pino Erwin

Denver

denise.erwin@bclplaw.com
+1 303 866 0631