BRESSLER, AMERY & ROSS

A PROFESSIONAL CORPORATION

INSURANCE LAW ALERT

JANUARY 2010

Obligations Of An Insurance Plan Administrator/ Employer Regarding Protected Health Information

Every employer offering a health plan to its employees and dealing with employees' protected health information ("PHI") is subject to certain obligations under the Standards for Privacy of Individually Identifiable Health Information ("Privacy Rule") enacted under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). HIPAA was implemented to develop stringent privacy protections for PHI and give patients certain rights over their PHI. Importantly, HIPAA has harsh penalties for violating its provisions, which were made even stronger by the recent American Recovery and Reinvestment Act of 2009 ("ARRA"). The ARRA added additional tiers to the penalty provisions. Now, the penalties are as follows:

- If an individual **did not know** they violated HIPAA, and by exercising reasonable diligence still would not have known, they are subject to $100 per violation with an annual maximum of $25K per year.
- The new penalty is where the violation is **due to reasonable cause** and not due to willful neglect, which subjects a company to a $1,000 penalty per violation with an annual maximum of $100K for repeat violations.
- If the violation is for **willful neglect**, but the violation is corrected, then the violator is subject to $10K per violation and an annual maximum of $250K.
- If the violation is due to **willful neglect** and the violation **is not corrected**, then the penalty is $50K per violation with an annual maximum of $1.5 million.

Importantly, HIPAA currently does not have an individual right of action, meaning an individual who has their PHI rights violated may not sue the violator under HIPAA.

Nevertheless, ARRA requires the U.S. Department of Health and Human Services ("HHS") to issue regulations in 2012 that allow individuals to receive a percentage of any civil monetary penalty or monetary settlement collected with respect to violations. Additionally, ARRA also authorizes state attorney generals to enforce HIPAA and allows for the recovery of attorney's fees.

To avoid the above-mentioned penalties, all employers who offer group health plans to their employees must be knowledgeable of HIPAA and the Privacy Rule. HIPAA applies to "covered entities", which includes "health plans." A health plan includes a group health plan, health insurance issuer, or a Health Maintenance Organization ("HMO"). Therefore, any employer offering a group health plan is a "covered entity" and must comply with HIPAA's requirements as outlined below. Additionally, beginning February 17, 2010, HIPAA will also apply to "business associates", which is any person or entity providing a service to a "covered entity" that has access to PHI.

Some of the most important Privacy Rule requirements include: creating a privacy policy and distributing a notice to a covered entity's enrollees identifying the privacy policy and the enrollees' HIPAA privacy rights (the "Notice"); designating a compliance officer within the covered entity; developing a complaint

procedure; creating sanctions for violation of the privacy policy; ensuring the covered entity's business associates comply with its privacy practices; and documenting any changes to the privacy policy.

Recently, new changes to HIPAA have been enacted. On November 21, 2009, the Genetic Information Nondiscrimination Act of 2008 ("GINA") became effective law. It authorizes HHS to enact new regulations that include genetic information within the definition of PHI, entitling it to all of the protections afforded to PHI under HIPAA.

Furthermore, under the Health Information Technology for Economic and Clinical Health Act ("HITECH Act"), not only will covered entities have to ensure that their business associates comply with HIPAA, but business associates must also do the same. The HITECH Act requires that if either the covered entity or a business associate becomes aware of a violation of the privacy practices, the non-breaching party must take reasonable action to repair the violation. If this proves unsuccessful, the non-breaching party must either terminate the contract or notify HHS.

Additionally, on September 23, 2009, a new notification requirement was enacted regarding breaches. Covered entities have until February 22, 2010 to begin to comply with the new requirements. In the event a covered entity determines a breach of an individual's PHI occurred, it must, within 60 days of discovering the breach, notify the individual, HHS, and, if the breach involved more than 500 individuals in one State, notify prominent media outlets serving the State. A breach occurs when there is a use or disclosure of PHI that compromises the security or privacy of the PHI. Notification will include: a description of what happened; the date of the breach and the discovery of the breach; the types of PHI that were involved; what the covered entity is doing to investigate; mitigate any harm to the individual; what the covered entity will do to protect against further breaches; and provide contact (telephone number, e-mail address, and website address) procedures for the individual to further inquire about the breach.

In conclusion, do not presume your privacy policy and/or business associate agreement is in compliance with HIPAA. HIPAA's requirements have drastically changed. Thus, to avoid harsh penalties, it is important to properly develop company PHI privacy policies and Notices that adhere to the law. The attorneys at Bressler, Amery & Ross, P.C. have experience in developing such policies and Notices and would be happy to discuss your company's particular situation. ■

For more information about any of the topics covered in this issue of the Insurance Law Alert, please contact:

Cynthia J. Borrelli, Esq.
cborrelli@bressler.com
973.966.9685

James P. Sasso, Esq.
jsasso@bressler.com
973.966.9682

BRESSLER, AMERY & ROSS

A PROFESSIONAL CORPORATION

17 State Street
New York, NY 10004
212.425.9300

325 Columbia Turnpike
Florham Park, NJ 07932
973.514.1200

2801 SW 149th Avenue
Miramar, FL 33027
954.499.7979

www.bressler.com