CLIENT ALERT

Brought to you by:

This is third in a series of Client Alerts centered on HIPAA and its importance to you.

Employers acting as the Group Health plan are a covered entity under HIPAA, as such you must have a way to encrypt and store any electronic data that contains the protected health Information (PHI) of your employees.

Symantec's 2016 Internet Security Threat Report estimated that over half a billion records were lost or stolen in 2015 due to data breaches. They also indicate that this is the proverbial tip of the iceberg as their research indicates that not all data breaches are reported as required. (https://www.symantec.com/content/dam/symantec/docs/infographics/istr-reporting-breaches-or-not-en.pdf)

Many employers forget that they have an obligation under HIPAA to protect the information that they receive from their employees. As an example, just because an employee emails you their enrollment form via normal email does not allow you to treat that form in the same manner. Any material that contains PHI in an electronic format must be housed on an encrypted drive and if you forward the form electronically, it must be done via secure email. Data breaches at the employer level are not as prevalent as the healthcare industry, but they do happen. Imagine the damage if the renewal census you prepare annually was hacked.

The Department of Labor is entering into their second round of HIPAA audits. Penalties for non-compliance have increased and penalties for willful non-compliance are severe. Attached is a summary of the four levels of possible penalties.

CHB Group has covered the topic of HIPAA extensively in Client Alerts over the years. Additional information can be found at www.chb-group.com, click on Client Alerts. Also visit www.chb.group and click on HIPAA in the Employee Benefits Resource Center.

You can also visit the government's website at: http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html or http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/index.html.

***DISCLAIMER* - This is high level information regarding HIPAA and is not meant to advise you of all your obligations under HIPAA, HITECT or the Omnibus Rule. This Client Alert is informational only and should not be construed as insurance, legal or tax advice. If you would like more information, please do not hesitate to contact our office, your legal counsel or accountant.**

QUICK HIPAA SUMMARY

HIPAA PRIVACY RULE
Defines protected health information (PHI), how entities may use it and what rights and protections consumers heave to view their PHI. Examples of PHI include, but are not limited to Name, Social Security Number, Address, and Health Information. PHI is any identifiable information.

HIPAA SECURITY
Outlines a covered entity's responsibilities to safeguard PHI in electronic form (e-mail, jump drives, computers, tablets, phones etc…) HIPAA Security Rules are designed to protect information from unauthorized access AND unauthorized use.

HITECH - The Health Information Technology for Economic and Clinical Health Act
HITECH established four penalty levels depending on knowledge, willful neglect and correction. It outlined situations under which HIPAA covered entities and business associates had to notify individuals of a security breach of unsecured PHI. When a security breach occurred there was a "harm threshold". If an entity believed that the harm threshold was not met, then no notification had to be made.

HIPAA OMNIBUS RULE
HHS felt that entities might have taken advantage of the ambiguous harm threshold under HITECH, by setting the bar high enough to avoid breach notifications. The Omnibus Rule eliminated the bar that was set under HITECT so any breach is now considered reportable. In addition, penalties were increased.

BELOW ARE THE FOUR PENALTY LEVELS:

Violation Category – From Section 1176(a)(1) of the Social Security Act	Each violation	All such violations of an identical provision in a calendar year
(A) The person did not know (and by exercising reasonable diligence would not have known) that they committed a HIPAA violation	$100 - $50,000	$1,500,000
(B) The violation was due to reasonable cause, but not willful neglect	$1,000 - $50,000	$1,500,000
(C)(i) The violation was due to willful neglect and steps were taken to correct the situation	$10,000 - $50,000	$1,500,000
(C)(ii) The violation was due to willful neglect and no steps were taken to correct the situation	$50,000	$1,500,000