CLIENT ALERT

Brought to you by:

HIPAA Reminder…

Fines can be severe if the Health and Human Services (HHS) Office for Civil Rights (OCR) determines that you have violated HIPAA

Up until now the major violators of HIPAA have been healthcare providers, insurers and ancillary suppliers like pharmacies. Few if any violations have been reported for Group Health Plans (GHP). However, this does not mean that GHPs are immune. Violations by Group Health Plans are subject to civil and criminal penalties.

We are providing this Client Alert as a reminder to our clients of your obligations under HIPAA and more recently The Health Information Technology for Economic and Clinical Health Act (HITECH).

HIPAA Refresher

PRIVACY - The Privacy Provision protects medical records and other Protected Health Information (PHI) maintained by Covered Entities. How and when health information may be used and released is limited based on the level of consent given by the patient or as permitted by HIPAA Regulations.

PHI is defined as any identifiable health information transmitted either electronically or otherwise. Some but not all PHI is defined as name, date of birth, address, medications, dates of provider service, Social Security number.

The Privacy Rule covers all forms of information whether written, electronic or oral.

SECURITY – The Security Rule only applies to PHI that is in electronic form, (ePHI). This may be data that is transmitted over the internet, stored on a computer or removable drive, CD, disk, tape, etc.

HITECH - was enacted as part of the American Recovery and Reinvestment Act on February 17, 2009. HITECH requires covered entities and business associates to provide notice of information security breaches affecting "unsecured protected health information" or "unsecured personal health record information," This act became effective on September 23, 2009**.**

WHAT DOES THIS MEAN FOR HUMAN RESOURCES?

First and foremost – Group Health Plans are covered entities, so every employer that sponsors a group medical/dental/prescription drug/vision plan is a covered entity.

As an HR representative, just about everything you touch that has to do with your group insurance includes PHI. According to some research, "a significant percentage of the U.S. population can be identified with just three key pieces of information, along with other publicly available data: gender, date of birth (Month/Day/Year), and 5 digit zip code." (*) **Think census data you send via e-mail to market your plans**

HITECH adds sharp teeth to HIPAA's Privacy and Security Rules. It also acknowledges that Business Associates must now take the same responsibility for securing PHI that covered entities have had.

Under the Security Rule, there are 27 Security Standards which incorporate 19 required implementation specifications and 23 addressable implementation specifications. These allowed a covered entity a fair amount of flexibility to show compliance with HIPAA Security. HITECH significantly restricts this flexibility and requires that covered entities add an additional layer of security to their electronic media**.**

Penalties for a breach of non-secured PHI can be staggering. HHS recently imposed a civil monetary penalty of $4.3 million for violations made by Cignet Health of Prince George's County.

WE URGE YOU TO MAKE SURE THAT YOU HAVE REVIEWED THE HIPAA REGULATIONS AND ARE ABIDING BY THEM. FOR ADDITIONAL INFORMATION, VISIT THE HEALTH AND HUMAN SERVICES WEBSITE AT www.hhs.gov/ocr/privacy/index.html
YOU MAY ALSO GO TO OUR WEBSITE, www.chb-group.com, AND UNDER **EMPLOYEE BENEFITS RESOURCE CENTER**, CLICK **HIPAA.**

(*) Golle P. (2006). Revisiting the Uniqueness of Simple Demographics in the US Population. Available at http://crypto.stanford.edu/~pgolle/papers/census.pdf

DISCLAIMER: ***This e-mail/Client Alert is informational only and is not meant to advise you of your entire obligation under the Privacy Act, Security Act and HITECH under HIPAA. This information is not considered insurance, legal or tax advice.***

If you would like more information, please do not hesitate to contact our office or your legal counsel.

SOME SUGGESTIONS:

BUSINESS ASSOCIATE AGREEMENTS (BAA) - Group health plans that share PHI with their business associates must obtain "satisfactory assurance" that their business associate will safeguard their enrollees' PHI. This is accomplished by executing a written contract or contract amendment with their business associates. This agreement contractually obligates the business associate to protect the PHI that they create, receive, use or disclose. Make sure you have a Business Associate Agreement with any business associate you use. (**As a service to our clients, we provided a BAA and have on file the executed agreements)**

HITECH looks at Data at Rest, Data in Motion and Data Disposed

For Data at Rest – Partition your hard drive and add encryption programs to one partition so that all documents that contain PHI are housed in that partition or use an offsite encrypted drive. Use encryption software for laptops, jump drives and any other removable drive/disk that contain PHI.

Data in Motion - Purchase an e-mail software program that meets AES (advanced Encryption Standard) encryption. These programs are readily available and do not require that the receiver have the same program or key. Make sure the one you use allows for sending and encrypting attachments. **Remember that an unencrypted e-mail is like sending a postcard through the mail.**

Data Disposed
Paper, CDs – Shred or destroy so that PHI cannot be read or reconstructed.
Electronic Media – Cleared, purged or destroyed consistent with NIST guidelines for media sanitation (www.csrc.nist.gov) such that PHI cannot be retrieved.

A note on Passwords – Do not think that just because your computer or document is password protected that you have met with HIPAA standards. There are programs that will crack a password by brute-force (trying every possible combination). A really fast computer can try 15 million passwords per second. It's possible for a 6 digit password to be hacked in less than an hour.

HIPAA Authorizations – Employees who come to you with claim issues should complete a HIPAA Authorization. This protects you from anyone claiming that you were unauthorized to have that information. A better alternative is to have your employee contact us directly. CHB Group will also require the completion of a HIPAA Authorization before we assist your employees.

DISCLAIMER: ***These suggestions are not meant to provide you with full compliance information under HIPAA.***

If you would like more information, please do not hesitate to contact our office or your legal counsel.