CLIENT ALERT

Brought to you by:

HIPAA INFORMATION FOR ALL EMPLOYERS THAT OFFER/SPONSOR HEALTH INSURANCE PLANS

Data breaches continue to occur at every level, from the mega store to the small privately owned pharmacy. The Federal Trade Commission provides a guide, *Start with Security, A Guide for Business*. This guide provides information on 10 vital areas for businesses to review against their own privacy and security practices, including:

- Start with security
- Control access to data sensibly
- Require secure passwords and authentication
- Store sensitive personal information securely and protect it during transmission
- Segment your network and monitor who's trying to get in and out
- Secure remote access to your network
- Apply sound security practices when developing new products
- Make sure your service providers implement reasonable security measures
- Put procedures in place to keep your security current and address vulnerabilities that may arise
- Secure paper, physical media and devices

Don't stop reading here because you think this doesn't apply to you – Every employer that sponsors a group health plan must be compliant with HIPAA. The level of personal information you maintain on your employees will determine just how compliant you need to be.

By way of reminder, on January 17th, 2013, the U.S Department of Health and Human Services (HHS) released the final ruling for HIPAA called the HIPAA Omnibus Rule. The Final Rule was effective on March 26, 2013, and HHS allowed covered entities and business associates 180 days from the effective date to become compliant with most of the provisions.

The Omnibus Rule is over 500 pages that consist of a set of complex and detailed regulations outlining the changes to the HIPAA Privacy Rule, HIPAA Security Rule, HIPAA Breach Notification Rule, and HIPAA Enforcement Rule (HIPAA and HITECH).

All Covered Entities and Business Associates Need to Comply with HIPAA

Business Associates Are

- anyone who works with a Covered Entity and Protected Health Information

This means CHB Group

Covered Entities Are:

- Healthcare Providers
- Employer Group Health Plans
- Health Insurance Companies
- Healthcare Clearing Houses

This means you

While HIPAA legislation was geared toward healthcare providers and insurers, a Group Health Plan is a covered entity. Penalties are severe for an employer who fails to comply out of "willful neglect"

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.

Consider:

Data at Rest – Where the data sits on your hard drive, jump drive, tablet, phone etc
Data in motion – How you send data that contains PHI
Data Destroyed – Destruction must meet NIST guidelines for media sanitation

ONLINE RISK ASSESSMENT - The HIPAA Security Rule requires that covered entities conduct a risk assessment of their organization. Health Plans are considered covered entities so when you act on behalf of the Health Plan you are a covered entity. If you haven't already addressed the Security Standards – You should do so immediately and on a regular basis. A risk assessment helps you ensure that you are compliant with HIPAA's administrative, physical, and technical safeguards as well as identifies any potential risks.

This security risk assessment (SRA) tool will help you conduct a risk assessment of your practices within the human resources department. Though this tool was designed mainly for health care offices, covered entities that must comply with HIPAA include Health Plans and Business Associates and may use it as well. This site includes a downloadable tool as well as instructional videos

HITECT – Health Information Technology for Economic and Clinical Health Act

HITECH added sharp teeth to HIPAA's Privacy and Security Rules and outlined situations under which HIPAA covered entities and business associates must notify affected individuals of a security breach of unsecured PHI. When a security breach occurred there was a "harm threshold" that had to be evaluated. If an entity believed that the harm threshold was not hit, then no notification had to be met. HHS felt that entities may have taken advantage of an ambiguous harm threshold setting the bar high enough to avoid breach notifications.

HIPAA OMNIBUS RULE – Eliminated the bar that was set under HITECT so any breach is now considered reportable. In addition, penalties were changed to range from $100-$50,000 with a maximum of $1.5 Million depending on knowledge, willful neglect and correction.

HOW CHB GROUP CAN HELP

We offer HIPAA Training Courses for employees of our clients. You will be able to assign courses and track which of your employees have started, completed, or not started their course(s). Contact us to your HR Staff employees started and trained.

We have covered HIPAA extensively in Client Alerts over the years. Additional information can be found on our website.

You may also access the government's website for additional information.

*DISCLAIMER - This is a high level summary 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, y**our legal counsel or accountant.***