CLIENT ALERT

Brought to you by:

PLEASE READ

TIME SENSITIVE MATERIAL

While all eyes have been watching the progress of Healthcare Reform, September 23, 2013 has slowly crept up on us. This is the day for final compliance of the HIPAA Omnibus Rule.

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 has 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) . For those of you that haven't read the 500 + pages, below is a summary of some of the more important pieces for sponsors of group health plans.

HIPAA AND HITECH REFRESHER

All Covered Entities and Business Associates Need to Comply with HIPAA
Covered Entities Are:

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

This means you!!!

[CHB Group comment - on the whole the HIPAA legislation was geared toward healthcare providers and insurers however make no mistake that a Group Health Plan is a covered entity. The new Rule provides severe penalties for an employer who fails to comply out of "willful neglect"]

Business Associates Are

- anyone who works with any of the above and receives PHI

This means CHB Group

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 etc
- Data in motion – How you send data that contains PHI
- Data Destroyed – Destruction must meet NIST guidelines for media sanitation

[CHB Group comment – at minimum, HR departments should have a way to send e-mails in a secure and encrypted fashion and all employee data, like census data should be housed on an encrypted drive]

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.

[CHB Group comment – Safeguarding PHI relies on the individuals who have access to PHI to consistently and correctly apply the security standards. So while 10% of safeguards are technical, the other 90% rely on individuals following rules and standards.]

This is a very brief summary of HIPAA Privacy, Security and HITECH. CHB Group has covered these topics extensively in Client Alerts over the years. Additional information can be found at www.chb-group.com, click on Client Alerts. Also visit: http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html

Below are some of the more significant pieces of this legislation. How the HIPAA Omnibus Rule applies to Group Health Plans:

CHANGES TO THE HIPAA PRIVACY RULE - Multiple privacy issues related to the use and disclosure of PHI are addressed in the final rule.

1. Marketing Communications – Not likely to affect Group Health Plans – a covered entity must obtain authorization from individuals before using or disclosing PHI for marketing communication that involve remuneration.
2. Authorizations – Not likely to affect Group Health Plans
    a. Research Authorizations must be study specific
    b. Further limits the use and disclosure of PHI for marketing and fundraising purposes, and prohibit the sale of protected health information without individual authorization
3. Notices of Privacy Practices (NPP) – Does affect Group Health Plans where PHI is received, NPPS must be updated to include
    a. The sale of PHI and the use of PHI for paid marketing requires an individual's authorization
    b. That any other disclosure of PHI not listed in the NPP will only be made upon an individual's authorization
    c. A statement that if a breach of unsecured PHI occurs that the individual has a right to be notified
    d. A health plan that intends to use or disclose PHI for underwriting purposes must state that the health plan is prohibited from using or disclosing genetic information for underwriting purposes.

CHANGES TO THE HIPAA SECURITY RULE

1. Business Associates and their sub-contractors must be fully compliant with HIPAA Security Rule. Business Associate Agreements must be in place and brought up to date for the new Rule. This affects Group Health Plans since the majority have at least one BA, and most have more than one.

    a. Examples of BA's under the expanded definition provided in the Final Rules
        1. Brokers/Consultants
        2. COBRA Administrators
        3. TPA's (medical and FSA)
        4. Health Advocates
        5. Online Enrollment Partners
2. Covered entities are required to provide individuals with access to PHI that is maintained in electronic form in the electronic form and format that is requested by the individual.
3. Both Covered Entities and Business Associates must ensure that their security safeguards are reasonable and appropriate.

CHANGES TO THE HIPAA BREACH NOTIFICATION RULE

1. HITECH outlined the when, the who and the how a breach notification had to be made. It also defined the Harm Threshold under which a covered entity or business associate could determine that no breach was made.
    a. The Final rule re-defines a breach so that any impermissible use or disclosure of PHI based on HIPAA is presumed to be a reportable breach.
    b. The Final Rule eliminates the Harm Threshold for a more stringent definition of breach which include four factors that need to be evaluated:
        1. the nature and extent of the PHI
        2. The nature of the unauthorized person who either used or received the PHI
        3. If the PHI was actually used or viewed
        4. If there are any mitigating factors
    c. The burden of proof is on the entity that no breach occurred based on a Risk Analysis using the four factors outlined above.
2. The evaluation must be documented and the outcome must be that there was a low probability that the information was compromised.
3. Covered Entities are required to notify HHS of all breaches of unsecured PHI affecting fewer than 500 individuals not later than 60 days after the end of the calendar year in which the breach was discovered.

CHANGES TO THE HIPAA ENFORCEMENT RULE

1. Penalties can range from $100 to $50,000 per violation depending on the level of culpability
2. There are four categories and four corresponding penalty amounts
    a. Individual did not know (and by exercising reasonable diligence would not have known) that he/she violated HIPAA
    b. HIPAA violation due to reasonable cause and not due to willful neglect
    c. HIPAA violation due to willful neglect but violation is corrected within the required time period
    d. HIPAA violation is due to willful neglect and is not corrected
3. There is a maximum penalty of $1.5 million for all violation of an identical provision

CHANGES TO BUSINESS ASSOCITES – Since the Privacy Rule, where applicable and the Security Rule now fully apply to Business Associates and and sub-contractor that they use, Group Health Plans should review their Business Associate Agreements as well as their business associates' practices to ensure that the business associates are complying fully with HIPAA. Completion of a Business Associates Agreement is the responsibility of the group health plan AND the business associate.

BEST PRACTICES:

1. If required – Revise your Notice of Privacy Practice – Only for Group Health Plans that receive PHI other than for enrollment. If your group health plan is a fully insured plan and does not receive PHI as part of a renewal, a Notice of Privacy Practice is not normally necessary
2. If required – Revise your Business Associates Agreements
3. If you haven't already addressed the Security Standards – Do so immediately. Please see NOTE below regarding e-mails we receive.
4. Update policies and practices to ensure compliance
5. Implement policies for sending and housing ePHI
6. Visit the Client Alert section of our website, www.chb-group.com for additional information regarding HIPAA and HITECH, or visit the HHS site, http://www.hhs.gov/ocr/privacy/index.html

NOTE: If we receive an unencrypted e-mail from you that based on specific criteria appears to contain PHI – be prepared to receive the following automatically generated e-mail in response.

THIS IS AN ELECTRONICALLY GENERATED E-MAIL

Dear Addressee:

CHB Group received an e-mail from you that included words or documents that based on certain criteria suggests that the e-mail contained Electronic Protected Health Information (ePHI) as defined by HIPAA. This e-mail was either not encrypted or was not sent via a secure connection. Depending on the information transmitted this e-mail may not meet the HIPAA Security Standards for the protection of electronic Protected Health Information and may be in violation of the HIPAA Security Rule.

We urge you to review your procedures regarding electronic transmission of Protected Health Information to make sure that you are in compliance with HIPAA Regulations. Additional Information can be found at the following websites:

http://www.chb-group.com/hipaa_chb_group.html

http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html

http://www.cms.gov/HIPAAGenInfo/04_PrivacyandSecurityStandards.asp#TopOfPage

DISCLAIMER ***- NOTE – as previously mentioned the new rule is over 500 pages. There is no way to summarize all the salient parts of this rule in 5 pages. This is a very 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, your legal counsel or accountant.***