CLIENT ALERT

Brought to you by:

The **Health Information Technology for Economic and Clinical Health Act** (HITECH)

substantially expands a Covered Entity's (1) responsibility under HIPAA's Privacy and Security Rules. HITECH also requires that Business Associates (2) comply with the law. **Group Health plans ARE covered Entities.**

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.

BUSINESS ASSOCIATE AGREEMENTS - 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.

---

(1) A Covered Entity is all health care providers who transmit health information electronically, Health Plans and Health Care Clearing Houses.

(2) A Business Associate is an entity that assists a covered entity with payment or operations and/or have access to the covered entity's protected health information (PHI)

HITECH

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 becomes effective on **September 23, 2009, however penalties are not likely to be imposed until after February 22, 2010.**

What is HITECH?

HITECH outlines the situations under which HIPAA covered entities must promptly notify affected individuals of a security breach of unsecured PHI, as well as the HHS Secretary and the media in cases where a breach affects more than 500 individuals. The regulations also require business associates of covered entities to notify the covered entity of breaches at or by the business associate.

What constitutes a Security Breach?

A security breach is the unauthorized acquisition, access, use or disclosure of protected health information.

What is secured PHI as opposed to unsecured PHI?

Secured PHI is defined as PHI where technologies and methodologies have been used that render it unusable, unreadable, or indecipherable to unauthorized individuals. Acceptable technologies/methodologies are: **Encryption and Destruction**

> **Encryption:**Electronic PHI has been encrypted as specified in the HIPAA Security Rule by 'the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key' [45 CFR 164.304, definition of 'encryption'] and such confidential process or key that might enable decryption has not been breached. To avoid a breach of the confidential process or key, these decryption tools should be stored on a device or at a location separate from the data they are used to encrypt or decrypt.
>
> **Destruction:**The media on which the PHI is stored or recorded has been destroyed in one of the following ways:
>
> > (i) Paper, film, or other hard copy media have been shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed. Redaction is specifically excluded as a means of data destruction.
> >
> > (ii) Electronic media have been cleared, purged, or destroyed consistent with NIST Special Publication 800-88, Guidelines for Media Sanitization [available at http://www.csrc.nist.gov], such that the PHI cannot be retrieved."

IN ENGLISH PLEASE!!!!

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." (3) (think census data 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.

The existing 27 Security Standards incorporate 19 Required implementation specifications and 23 Addressable implementation specifications. This allowed a covered entity a fair amount of flexibility to show compliance with HIPAA Security. (4) HITECH significantly restricts this flexibility and requires that covered entities add an additional layer of security to their electronic media**.**

Penalties for a breach in non-secured PHI can be as high as 1.5 million dollars. If there is a security breach, but the information was secured as defined by HITECH, there is no penalty.

DISCLAIMER: *This e-mai/Client Alert is informational only and is not meant to advise you of your entire obligation under the Privacy, Security Acts 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:

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.

Laptops, jump drives and any other removable drive/disk that contain PHI – Use encryption software.

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. If someone really wants to read it – it can be done.**

Data Disposed
Paper, CD,s – Shredding or destroy so that PHI cannot be read or reconstructed.
Electronic Media – Cleared, purged or destroyed consistent with NIST guidelines for media sanitation (5) such that PHI cannot be retrieved.

A note on Passwords – There are programs that a hacker can buy that will crack a password by brute-force (trying every possible combination). A really fast computer can try 15 million passwords per second. **A 6 digit password can be cracked in 1 hour or less by a hacker.**

Business Associates Agreements (BAA) – Under Pre-HITECH HIPAA, it was the responsibility of the covered entity, (i.e. Group Plan) not the business associate to make sure a BAA was in place. As a service to our clients, we provided a BAA and have on file the executed contracts (some date back to 2003). After February of 2010, the onus for an executed BAA will be held jointly by the covered entity and the business associate.

HIPAA Authorizations – Effective immediately, before we assist anyone with a claim issue we will ask that the claimant complete a HIPAA Authorization. If the claimant is going through the HR rep, we recommend that the HR rep be named in the authorization. Faxed copies will be accepted.

---

(3) Information taken form 4/27/09 Federal Register Vol. 74, No. 79. (www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/guidance_breachnotice.html)
(4) See Links at end of Alert for assistance with the Security Standards
(5) www.csrc.nist.gov

HELPFUL LINKS

PRIVACY STANDARD LINKS
www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html

SECURITY STANDARD LINKS
www.cms.hhs.gov/EducationMaterials/04_SecurityMaterials.asp#TopOfPage

HITECH
www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/breachnotificationifr.html

www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/guidance_breachnotice.html

OTHER SITES

www.hipaa.org

www.hhs.gov

www.hipaa.com

www.nist.gov/index.html

DISCLAIMER: *These website links are to be viewed at the viewer's risk. CHB Group cannot confirm the veracity of the information provided on these sites.*