CLIENT ALERT

Brought to you by:

Results of the Office of Civil Rights HIPAA Audits

During 2016, OCR as part of its continued efforts to assess compliance with the HIPAA Privacy, Security and Breach Notification Rules, randomly selected certain covered entities and business associates for audits. These audits were used to determine the level of compliance for the policies and procedures adopted and employed by covered entities and their business associates to meet the standards and implementation specifications of the Privacy, Security, and Breach Notification Rules.

When you act as the Plan Sponsor for a Group Health Plan you are considered a COVERED ENTITY, so you are subject to HIPAA

The results of these audits were concerning in that OCR rated the auditees compliance with the HIPAA Privacy, Security and Breach Notification standards as largely "inadequate," with over 94% of the covered entities failing to demonstrate appropriate risk management plans.

Don't' Wait - Prepare Now!!!

The Federal Trade Commission recently released ***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. https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf

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 now! A risk assessment helps you ensure that you are compliant with HIPAA's administrative, physical, and technical safeguards.

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 mainly designed for health care offices, covered entities that must comply with HIPAA include Health Plans and Business Associates and may use it as well. Visit the following site for additional information and to download the tool.

http://www.healthit.gov/providers-professionals/security-risk-assessment

Two Areas Where most employers fail HIPAA Security

In our experience there are two main areas where employers have not made changes to adequately protect ePHI, where ePHI is electronic Protected Health Information and is defined as ANY identifying information.

- The first is not having a way to send encrypted emails
- The second is not having an encrypted drive where documents with ePHI are housed. (census data, enrollment forms, claim issues, etc…).

Note that the HIPAA Security regulations are extensive and these are only two issues that we encounter often. Having an encrypted drive and emails does not by itself guarantee that you would pass an audit.

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