CLIENT ALERT

Brought to you by:

OCR Launches Phase 2 of HIPAA Audit Program

As a part of its continued efforts to assess compliance with the HIPAA Privacy, Security and Breach Notification Rules, the HHS Office for Civil Rights (OCR) has begun its next phase of audits of covered entities and their business associates. Audits are an important compliance tool for OCR that supplements OCR's other enforcement tools, such as complaint investigations and compliance reviews. These tools enable OCR to identify best practices and proactively uncover and address risks and vulnerabilities to protected health information (PHI).

Don't stop reading here because you think this does not apply to you – it does if you sponsor a group health plan

In its 2016 Phase 2 HIPAA Audit Program, OCR will review the policies and procedures adopted and employed by covered entities and their business associates to meet selected standards and implementation specifications of the Privacy, Security, and Breach Notification Rules. These audits will primarily be desk audits, although some on-site audits will be conducted.

When you act as the Plan Sponsor for a Group Health Plan you are considered a COVERED ENTITY

The 2016 audit process begins with verification of an entity's address and contact information. An email is being sent to covered entities and business associates requesting that contact information be provided to OCR in a timely manner. OCR will then transmit a pre-audit questionnaire to gather data about the size, type, and operations of potential auditees; this data will be used with other information to create potential audit subject pools.

If an entity does not respond to OCR's request to verify its contact information or pre-audit questionnaire, OCR will use publically available information about the entity to create its audit subject pool. Therefore an entity that does not respond to OCR may still be selected for an audit or subject to a compliance review. Communications from OCR will be sent via email and may be incorrectly classified as spam. If your entity's spam filtering and virus protection are automatically enabled, we expect entities to check their junk or spam email folder for emails from OCR.

The audit program is developing on pace and OCR is committed to transparency about the process. OCR will post updated audit protocols on its website closer to conducting the 2016 audits. The audit protocol will be updated to reflect the HIPAA Omnibus Rulemaking and can be used as a tool by organizations to conduct their own internal self-audits as part of their HIPAA compliance activities.

OCR's audits will enhance industry awareness of compliance obligations and enable OCR to better target technical assistance regarding problems identified through the audits. Through the information gleaned from the audits, OCR will develop tools and guidance to assist the industry in compliance self-evaluation and in preventing breaches. We will evaluate the results and procedures used in our phase 2 audits to develop our permanent audit program. http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/phase2announcement/index.html

What are your next steps?

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 areas 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.

There is another area that we are actively working on updating on our end. **You must have a Business Associates Agreement with each Business Associate that you deal with.** Because we handle your enrollments, billing issues, claim issues, etc…CHB Group is one of your Business Associates. Since HIPAA became effective, we have had our clients execute these agreements several times over the years in keeping with required updates.

Periodically, we believe it is prudent to request the execution of a new set, due to legislative changes or turnover at the client level. In light of this new phase of audits, we are requesting that all of our clients execute a new Business Associate Agreement with us. Within the next week, you will receive a new Business Associate Agreement (if you haven't already), please promptly sign and return the agreement and keep your copy in a place that is readily available should you get audited. Note that having valid Business Associate Agreement is a HIPAA requirement of the covered entity. Do not wait for your other business associates to come to you, make sure you have them in place with all of your business associates.

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

***DISCLAIMER* - This is high level information regarding HIPAA 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.**