CLIENT ALERT

Brought to you by:

HHS releases security risk assessment tool to help covered entities with HIPAA compliance

The Health Insurance Portability and Accountability Act (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. This is not a new topic, but one that bears repeating…HR departments are just as much at risk for HIPAA Security breaches and penalties as medical practices and insurance companies.

A risk assessment helps you ensure that you are compliant with HIPAA's administrative, physical, and technical safeguards. This requirement dates back to when HIPAA Security came into law, but up until now was difficult to assess.

This new 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 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

Instances where you are at risk:

1. Sending employee information via unsecured e-mail, such as names, date of birth, salary information, Social Security numbers and addresses.
2. Sending enrollment forms via unsecured e-mail.
3. Sending Claim Forms, Provider Bills, EOBS via unsecured e-mail.
4. Sending Census Data via unsecured e-mail.
5. Having a laptop, jump drive, tablet, smartphone etc… that you house employee information on that is unsecure.
6. Using an unsecured wi-fi connection when sending information

HIPAA requires that any electronic PHI (ePHI) must be sent and housed securely. This means encrypted. At CHB Group we take the safeguarding of your employees' information very seriously. We use encrypted e-mail to send anything containing PHI and all ePHI (claims assistance requests, electronic enrollment forms, census data etc.) is housed on a secure, encrypted cloud drive.

Below is short summary from our CLIENT ALERT dated 5/20/2011. The full Client Alert can be viewed on our website, www.chb-group.com, Click Client Alerts and then on 5/2011 HIPAA REMINDER

- 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 or use an offsite encrypted drive. Use encryption software for laptops, jump drives and any other removable drive/disk that contain PHI.
- 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 through the mail.
- Data Disposed - Paper, CDs – Shred or destroy so that PHI cannot be read or reconstructed.
- Electronic Media – Cleared, purged or destroyed consistent with NIST guidelines for media sanitation (www.csrc.nist.gov) such that PHI cannot be retrieved.
- Password protecting a computer or document does not meet the HIPAA standards for safeguarding data.
- You must have a Business Associates Agreement in place with any entity that you share ePHI with – your broker, COBRA or FSA Administrator, Health Advocate etc…

DISCLAIMER: ***This e-mail/Client Alert is informational only and is not meant to advise you of your entire obligations under the Privacy Act, Security Act 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.