CLIENT ALERT

Brought to you by:

The US is facing unprecedented cyber/ransomware attacks. These attacks are no longer focused on highly regulated industries or industry giants. Every corporation should ensure that they are taking steps to protect against cyberattacks – Including your insurance broker. Insurance brokers that do not protect against such attacks will put both their clients at risk and their clients' employee data at risk.

We actively assess our systems to ensure that the information you and your employees share with us is safe. How CHB protects itself and your data from cyberattacks:

Question – What would happen if there was a Ransomware attack on your systems?
Answer - Our Server and Emails are backed up each night to an offsite encrypted location. Every computer is backed up each night to an onsite encrypted server. Three portable hard drives are used in rotation to backup this server and two are always off site. This means that if our server or a computer is hacked, we can reload all the data within a very short time frame.

Question - If your systems were hacked, what happens to the data that you store regarding my employees, such as enrollment and claim information?
Answer - Data that contains ePHI (Electronic Personal Health Information) is housed on a regularly backed up 256-byte encrypted cloud drive in compliance with HIPAA. This data is unreadable to a hacker without the encryption key.

Question – Are you fully HIPAA compliant?
Answer – Yes, we are and we work to ensure that our clients are as well. Brokers are considered a Business Associate (BA) of the employer under HIPAA and therefore must be fully HIPAA compliant. Below are just some of what we do to stay compliant:

1. We ensure that there is an up-to-date Business Associates Agreement (BAA) between ourselves and our clients and any downstream BAs, like COBRA vendors. BAAs are required under HIPAA and fines may be levied on both the employer and the Business Associate if one does not exist. [1]
2. We use ZixCorp to send encrypted emails that contain personal information. Sending such information unencrypted is a HIPAA violation that must be reported to the Department of Health and Human Services (HHS). [2]
3. We use a cloud drive that meets HHS requirements for encryption to house all documents that contain personal information. [3]
4. We perform a risk analysis and risk management plan annually as required by HIPAA based on the outcome of this analysis, if necessary, practices and procedures are modified.

[1] $1.55 million settlement underscores the importance of executing HIPAA business associate agreements | Guidance Portal (hhs.gov)
[2] Breach Reporting | HHS.gov
[3[https://www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html