# CLIENT ALERT

**Brought to you by:**

**The Hospice of North Idaho (HONI) has agreed to pay the U.S. Department of Health and Human Services' (HHS) $50,000 to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule. This is the first settlement involving a breach of unprotected electronic protected health information (ePHI) affecting fewer than 500 individuals…**

**This involved a stolen laptop with information regarding 441 patients and their protected health information.**

**<u>This is not a new topic, but one that bears repeating…Human Resource departments are just as much at risk for HIPAA Security breaches and penalties as medical practices.</u>**

**Instances where you are at risk:**

1. **Sending employee information via unsecured e-mail, such as names, date of birth, SS#, address**
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 unsecure wi-fi connection to send information**

**HIPAA requires that any electronic PHI (ePHI) must be sent and housed securely. <u>This means encrypted</u>. Sending an excel spreadsheet that is password protected does not meet the HIPAA standards of protecting ePHI.**

**Attached is a one page flyer from the Department of Health and Human Services regarding safeguarding data on mobile devices.**

**At CHB Group we take the safeguarding of your employees information very seriously. We use encrypted e-mail to send anything that contains PHI and all ePHI (claims assistance requests, electronic enrollment forms, census data etc..) is housed on a safe, secure, encrypted cloud server.**

**Below is an excerpt 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**

**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 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.

**A note on Passwords – Do not think that just because your computer or document is password protected that you have met with HIPAA standards. There are programs that will crack a password by brute-force (trying every possible combination). It is possible for a 6 digit password to be hacked in less than an hour.**

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

**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.***