14 boring (but really important) things you should know to keep your HBPA affiliate HIPAA compliant

The 1996 Health Insurance Portability and Accountability Act (HIPAA) has seen major updates since its inception with change being the only constant. HIPAA has been a topic we have talked about several times since the 2002 Winter Convention. Now is a good time to review your affiliates HIPAA compliance. If you have the following documents and procedures in place, that's great. You may find that you have informal (undocumented) policies and procedures that your staff follows. If so, now is the time to get those formalized. If HIPAA compliance is not ranked among your top priorities at any given moment in the day, it should be. Not only will it keep your affiliate safe, but you will be compliant with your own ethical mandate to maintain your horsemen's protected personal health information a in both a secure and reliable manner. Recently the Department of Human Health Services served notice that it was increasing audits and enforcing fines. True to its word, staggering fines are being levied against companies that fail to comply with HIPAA regulations.

1. Somebody Needs to Be in Charge of Compliance

Have a Privacy Officer. Individuals have a variety of rights under HIPAA; make sure that someone in your office is in charge of administering and protecting those rights. There should be one person assigned the title of Privacy or HIPAA Compliance Officer who knows how HIPAA and HITECH applies to your office setting. Failure to comply with these laws may expose your affiliate to increased liability, mandated government audits, and lawsuits for non-compliance. These laws are enforced by the federal government's Office of Civil Rights. Classes to learn about compliance are available around the country; check on-line to locate a local seminar conducted by a national company.. Classes are also available on-line.

2. Security Awareness

Once a Privacy Officer is trained, it will be that person's responsibility to train and update every member of your office staff. Do not let your staff become complacent! Regularly review policies and conduct training. This is especially critical given new, more stringent HIPAA requirements, oversight & penalties. Keep current on HIPAA happenings and share information with your staff regularly. This should include programs for new hires, annual training, and periodic security reminders. It is crucial that you keep an audit trail of your reminders, document everything that you do. You may need that paper trail!

3. Risk Analysis

A risk analysis and management policy should be documented for how risks are identified and a process of response should a risk be encountered. Health information is one of the most important types of data and needs to be safeguarded. At a very high level, a process is needed to identify risks and the controls that are in place to mitigate them. Under HIPAA, the primary concern is risk to systems and processes that deal with health information, although it can be extended to any part of the organization. There are plenty of good online resources to assist in developing a risk analysis and management strategy. A well-

documented risk analysis and management program will include the process by which risks are identified, as well as the process for establishing and executing action plans in response.

4. Know that Your Biggest Security Threat Comes From Within

Do you have set guidelines for whom and who isn't allowed in your work area? If not, better start making a list now. This policy should include specifically who is and isn't allowed to physically enter your work space, sitting at staff desks and using company computers. Decide how this policy will be enforced? By far, the largest number of patient security threats are caused by, or enabled by, internal users, i.e. office, followed by nosey visitors to your office. Role-play regularly with staff on patient privacy scenarios and ensure you provide annual HIPAA training for your staff as that is considered a "best practice." Understand security no-no's. Never allow public e-mail systems; unsecured WiFi; outdated anti-virus and spam software when transferring protected personal health information.

5. Update your Business Associate Agreements (BBAs)

Beginning in September, 2013 covered entities will be required to have on file signed copies of the updated BBAs. Typically the following would be included on the list of those needing to sign the new BBA if they have access to protected personal health information either directly, indirectly or casually: Board Members, Staff Members, Volunteers, Staff Members of other Organization with which you may partner, Professional and Staff members of your Health Clinic, Substance Abuse Counselors, Chaplains, Accountants, Attorneys, IT Contractors, Janitorial Staff, and anyone else who may have access to your office space or protected personal health insurance.

6. Post your Notice of Privacy Practices.

Post on your website and have copies at the front desk. Make sure your Notice of Privacy Practices is current.

7. Access Control

There should be specific policies and procedures on how users are granted access to programs, sensitive data, or equipment. This needs to be documented in its own policy too! There may be different access levels of data, programs, and equipment which needs to be included in an access control policy. The policy should also include how access is authorized when requested, how administrators should disable accounts (if needed), and how records of all access activity is stored.

8. Have a secure password system

Protect security by avoiding 'weak' or shared user names and passwords. A login such as 'staff' invites abuse and patient security breaches. Employees should not write down their passwords or share them with other employees. The Privacy Officer should maintain a current list of all company passwords that access protected personal health information.

9. Media Disposal

A common concern is data that lives on equipment other than computers: copiers, smart phones, and fax-machines . Make sure that you have policies and procedures in place that mandate how you wipe the data off each kind of storage media and how these activities are logged. There may be a reliable media disposal firm in your area that will securely dispose of your outdated media and shred the hard drive. Don't forget to have a shredder in your office to destroy small amounts of confidential paperwork. You may also need to contact a commercial shredder for larger amounts such as boxes of old files.

10. Malicious Software
You should utilize an anti-virus software package and those who don't may be susceptible to spyware and malware. You must document virus definition updates and the frequency of updates needs to be tracked in addition to response procedures should a workstation become infected. Don't forget to include staff policies about opening viruses, detecting them, and reporting them. Be wary about opening attachments from unknown senders. Be sure not to disable the anti-virus software.

11. Workstation Use Policies
Be sure to log out of your workstation prior when leaving it unattended for a long period of time. Develop a policy that addresses computer access which includes the way login records are monitored, ability to change and reset passwords, and putting a limit on unsuccessful login attempts should be included for the company's sake.

12. Disaster Recovery
In the event of a disaster, companies should have a well thought out plan of what to do if a server crashes or if there is a power outage that prohibits productivity as well as where this plan can be easily accessed. Not only should this policy cover disaster recovery solutions it should also cover backup and storage policies, how often these procedures are tested, how they are identified and how everything will be restored after the disaster. Don't forget to include a policy on where the DR plan is stored so you can get it in the event of an emergency.

13. Business Continuity
As an extension of disaster recovery, your business continuity policy should indicate how business operations will continue after a disaster occurs in addition to personnel procedures, horsemen relations and communication, secondary work sites and the command structure. It is best to include all aspects of your affiliate from development to implementation for this policy.

14. Review and audit procedure
Every item on this list has a couple of things in common: First, it must be auditable. You don't get credit unless there is a documented audit log that shows that these procedures are being executed. There also needs to be a process that ensures that the policies and procedures are reviewed regularly. Now that you have gone over several policies; a policy needs to also oversee that these procedures are reviewed on a regular basis. But that's not all, should you come across something in a policy that needs to be updated, you can rest assure that you'll need a policy that addresses updates too.

Please keep in mind that these are only a few key policies that should be touched upon-there are many more. This is simply a good start to getting on your way to being HIPAA compliant and to safeguard your affiliate in the event of an audit.

National Benefit Providers Committee Meeting
July 12, 2013