ARRA Changes Rules for HIPAA – Did You Miss These Three February Deadlines?

With so much going on in healthcare, it would not surprise me if a lot of practices missed the February 2010 deadline for **three** expanded HIPAA rules. This expansion was dictated by the Health Information Technology for Economic and Clinical Health (HITECH) Act passed by Congress in February 2009.

If you haven't already, get started now with the new requirements.

1. **New obligations for business associates (BA) – February 17, 2010** Remember that a BA is a person or organization outside of your entity with whom you share protected health information (PHI) so they may provide services to you. Good examples are your billing service, collection agency, attorney, consultant, computer vendors, attorneys and providers of documentation abstracting or coding services. Under HITECH, BA have the same responsibilities for breaches as the healthcare entity does, but it is the healthcare organization's responsibility to have an updated, signed BA agreement in place that describes this new responsibility. **Here** is an excellent example of a BA agreement (first link under Publications) that you can download and tweak for your practice.
2. **New disclosure agreement provision – February 18, 2010** This is a big one! Patients now may waive their right to have you file their medical insurance, pay for your services themselves and request that their medical information NOT be disclosed to their insurance plan or any other entity. In other words, patients may elect to become "self-insured". I recommend that you create a

new financial class for these patients so they neither fall into the standard self-pay/financial assistance class or into their actual insurance class. These patients, if you have any, will need to be identified according to their wishes, which could mean that they want you to file insurance for some services and not for others. This means their record must be tagged for what records can be released and what records cannot. There could be an argument made either way for whether or not these patients should receive self-pay discounts that you have in place for your non-insured patients. I would be interested to know how different groups have decided to handle this. There are sample forms for PHI disclosure accounting and for patients to request an accounting of PHI disclosures in the Manage My Practice Library under Operations.

3. **Information breach notification – February 22, 2010**
   We've heard a lot about this one as the media (along with HHS) must now be notified if a PHI breach involves 500 people or more. Breaches are being reported weekly as non-encrypted laptops are stolen or repurposed, and as copier hard drives **(story here)** go unnoticed as a security risk. If a breach involves 500 people or less, each individual must receive written notice with details of the breach, the information disclosed, and the steps being taken by the practice or entity to avoid any future breaches, as well as explaining the rights of the patient(s) in protecting their private healthcare information. Several of my employees have received notification letters from health plans and they have been horrified that this could happen. Note that entities that secure health information through encryption or destruction don't have to provide notification in the event of a breach!

Enforcement is also beefed up.

Criminal penalties will apply to covered entities that violate

privacy rules AND to those organizations' individual employees (can you track who accesses whose records when?) Civil penalties have been increased and harmed individuals may share in the booty. Probably most importantly, HITECH gives state attorneys general the power to enforce HIPAA rules.

Other resources:

HHS FAQ on HIPAA Privacy

AMA HIPAA Resources

Healthcare Blog Listing