ARE YOU COMPLIANT WITH ALL HIPAA STANDARDS?
COULD YOU DEFEND AGAINST A COMPLAINT?

Significant HIPAA Changes Began in 2009 and will continue for years due to changes dictated by the American Reinvestment and Recovery Act of 2009 (ARRA). Health and Human Services has published new HIPAA regulations and guidance as a result of the HITECH Act which was a part of ARRA.

Just a few of the significant changes include new Breach regulations effective September 23, 2009; Business Associates became covered entities on February 17, 2010 requiring changes by practices and BAs; and the enforcement of HIPAA has been mandated and funded by Congress. The penalties are higher and mandatory in some cases.

Now is a good time to evaluate your level of compliance. Take a few minutes to go through a few questions. The questions do not represent all that is new or required but are examples of what is needed.

1. Have you trained all workforce members on the Privacy Rule and the Security Rule? HIPAA requires training when changes happen and to prove you are enforcing an active program. Do you have documentation of the staff training?
2. Are all new employees trained when hired?
3. Have you documented polices as directed by both the Privacy and Security Rules?
4. Do you have documented policies for the Breach regulations of 2009?
5. Do you have a written Risk Assessment for your practice that is updated annually? Mandated by the Security Rule.
6. Do you have a patient complaint process in place? Do employees know who to direct complaints to?
7. Do you retain copies of all privacy complaints and the results of the investigations? You are required to document the decision on breach for each and why you made that decision.
8. Do your authorization forms contain the required patient disclosure statements? An expiration date or event? The purpose of the requested release or use? No forms or inappropriate forms are one of the top 5 complaints.
9. Do you have a documented Sanctions Policy that will apply for any staff violations? Do you enforce it?
10. Does every employee have their own access code to the computer? Do you enforce the use? This is a mandatory requirement of the Security Rule.
11. Have you informed employees of what constitutes a security incident? Do they know how to report one?
12. Do you have an employee suggestion and complaint process and make employees aware of how to report potential issues they see?
13. The HITECH Act of 2009 substantially changed the HIPAA regulations. Have you adjusted your programs, policies and actions?

If you answered no to any of the above, you may find it difficult to defend against a complaint made by a patient or a disgruntled employee, even if the complaint is unfounded. At best you may find yourself having to submit a corrective action plan to the Office for Civil Rights (OCR) as a result.

TMC can keep you up to date on the latest information, document policies for you on the new regulations and share best practices on compliance with you. Read more about TMC HIPAA education and compliance programs to see how TMC can assist you as HIPAA regulations continue to change.