

HIPAA Compliance

HIPAA Compliance

PMAB complies with all HIPAA Regulation Mandates. The HIPAA "Standards for the Privacy of Individually Identifiable Health Information" are honored at PMAB and attention is paid to each new development

HIPAA News Federal HIPAA Regulation Mandates

Final privacy regulations were issued by the US Department of Health and Human Services for the HIPAA (Health Insurance Portability and Accountability of 1996) on August 14, 2000. HIPAA is the law right now. On April 14, 2003, penalties will be imposed to enforce compliance with the law. The HIPAA laws affect almost every healthcare provider. HIPAA will change the way all these practices do business. It defines that the information in client files belongs to the client, not the practice and MUST be protected. HIPAA will cause sweeping changes in the way that information is handled and protected. The HIPAA Privacy Rules require certain specific methods of handling the protected health information (PHI) of clients. On April 14, 2003, these changes must be implemented. Fines, penalties and possible jail time can be imposed for non-compliance. To be compliant, a practice must:

- Review the access employee's have to protected information and determine the "minimum necessary" access
- Develop specific policies and procedures regarding the HIPAA requirements.
- Provide training for current and all future employees on those policies and procedures.
- Appoint a privacy officer to monitor the practice's HIPAA compliance.
- Provide a Notice of Privacy Practices to all patients.
- Obtain HIPAA-compliant agreements with all business associates
- Get a signed Authorization every time patient information is released per request of a client. HIPAA doesn't stop there. It also requires new procedures regarding patient access to their information: New procedures must be implemented to provide patients:
 - Access to their medical information including providing copies at their request
 - Ability to make amendments their records
 - Accountings of any and all disclosures made of their medical information for any use other than treatment, payment and firm operations. And the practice must notify each patient of these rights with a "Notice of Privacy Practices." This notice must include the patient's rights, the practice's HIPAA policies and the address of where to complain.

And HIPAA laws do not override most restrictive state privacy laws. So your firm must be compliant with state AND federal privacy laws.

April 14, 2003, the penalties will be imposed. The fines are large enough to put a practice out of business. For a simple violation, such as not documenting release of protected health information in every client file affected, the fine is \$100 per standard violated, per client per year. The maximum fine per standard violated is \$25,000 per year. Suppose your firm had 3,000 clients and an employee neglected to put a copy of the transaction in half the files of your practice. The fine could be 1,500 patients times \$100, or \$150,000. And that is for ONE violation. What would the fine be for NOT being compliant at all? And for misuse of patient data the fine could be \$250,000 plus jail time.