

Overview of the Federal HIPAA Regulations

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, 2002. HIPAA is the law *right now*. The deadline for healthcare providers and large group health plans passed last April 14, 2003. Small group plans have until next April 14, 2004 to be compliant. Penalties can now be imposed to enforce compliance with the law.

The HIPAA laws affect almost every healthcare provider, all group medical insurance companies, HMO's and all group health plans with 50 or more eligible employees. (The regulations say 50 or more participants but does not define what is meant by "participants". The accepted definition is to count eligible employees not actual participants. Eligible means Cobra ex-employees and ALL other employees *that can elect the coverage whether they have taken it or not.*) HIPAA will change the way healthcare plan providers and sponsors (employers) do business. It will also affect how group health plans collect, retain and protect personal health information on employees. HIPAA defines that the health information in healthcare client and employee medical files belongs to the client/employee, and **MUST** be protected. HIPAA will cause sweeping changes in the way this information is handled and protected.

The HIPAA Privacy Rules require certain specific methods of handling the protected health information (PHI). On April 14, 2004, these changes must be implemented for small health plans. Fines, penalties and possible jail time can be imposed for non-compliance. To be compliant, an healthcare plan sponsor must:

- Provide information to employees about their privacy rights and how their information can be used.
- Adopt clear privacy procedures for its medical plan.
- Train healthcare administration employees so that they understand the privacy procedures.
- Designate an individual to be responsible for seeing that the privacy procedures are adopted and followed. (The Privacy Officer)
- Secure employee records containing individually identifiable health information so that they are not readily available to those who do not need see them.

HIPAA doesn't stop there. It *requires* the healthcare plan to:

- Have a HIPAA Policies and Procedures Manual. This manual must outline how the protected health information is handled, protected and used.
- The law also requires that *any* outside entities that have access to the employee medical information are agents of the health care plan and they are called business associates. Each Business Associate must sign a *Business Associate Agreement* guaranteeing they too will provide the same respect and protection of the information.

- And who is responsible for making sure the healthcare plan is HIPAA compliant? The plan sponsor usually referred to as the employer.
- The employer must notify each employee of his/her HIPAA rights with a "Notice of Privacy Practices." This notice must include their rights, the company's HIPAA policies and the addresses and contact information of where and whom to complain.
- And HIPAA laws do not override more restrictive state privacy laws. So your firm must be compliant with state AND federal privacy laws.

On April 14, 2004, penalties can be imposed on small health plans for HIPAA violations. The fines are large enough to be of serious consequences. For a simple violation, such as not documenting release of protected health information in every employee file, the fine is \$100 per standard violated, per employee per year. The maximum fine per employee per standard violated is \$25,000 per year. Suppose your firm had 100 employees and an employee neglected to put a copy of the transaction in half the files. The fine would be 50 employees times \$100, or \$5,000. And that is for ONE violation. What would the fine be for NOT being compliant at all? And for misuse of employee PHI the fine could be \$250,000 plus jail time. These fines do not include the costs for the employer to have to deal with the Office of Civil Rights for a full HIPAA audit to determine if there were violations and what they are.

HIPAA compliance is not an option. Just like COBRA, HIPAA is the law right now. Most covered entities had to be compliant by April 14, 2003. Small health plans have until April 14 of 2004.

How easy is it to face a HIPAA audit? Real easy. ANYONE can turn a covered entity into the Health and Human Services or the enforcement division, the Office of Civil Rights. Ever had an unhappy employee leave or experience the anger of a dissatisfied customer? One simple call or post card can bring any employer or other covered entity to the attention of the Health and Human Services' Office of Civil Rights.

Dennis P. Begley CLU ChFC
ER.HIPAAps.com