

HIPAA & YOUR BUSINESS ASSOCIATES

DID YOU KNOW that you could be fined based on the practices of your business associates? Any business associates who receives your patient's Protected Health Information (PHI) is subject to all Health Insurance Portability and Accountability Act (HIPAA) regulations. Your billing service, telephone answering service, accounting firm and collection agency, to name a few, all must now be HIPAA compliant.

This significant expansion of HIPAA is the result of the Health Information Technology for Economic and Clinical Health (HITECH) Act passed by the United States Congress in February 2009.

The HITECH Act Security Rule requires reasonable assurance of the confidentiality, integrity and availability of Electronic Protected Health Information (ePHI) in three key elements:

- ❖ **Administrative Safeguards** security management process, security personnel, information access management, workforce training and management and evaluation.
- ❖ **Physical Safeguards** facility access and control, workstation and device security.
- ❖ **Technical Safeguards** access control, audit controls, integrity control and transmission security.

Failure to comply with the HITECH and HIPAA regulations can cause severe financial penalties reaching up to \$1.5 million for you and your practice.

www.ama-assn.org/amednews

If your office becomes aware of a HIPAA breach made by your business associate, you are required to take reasonable steps in correcting the violation. In the event that such steps are unsuccessful, then you must terminate your business associate agreement.

To avoid terminating contracts or securing other business associates, we highly recommend surveying your business associates' HIPAA compliance processes.

Examples to ask:

What are your policies and procedures protecting against the use or disclosure of PHI?

Has your staff received training from a HIPAA professional?

Are all vendors associated with your business associates HIPAA compliant?

Do you have all of the necessary resources to remain HIPAA compliant?

