



www.medsafe.com

5 Steps to Avoid a Fine for a Breach of PHI

With over 600 major breaches of health care information reported to federal authorities since the HIPAA breach notification rule went into effect in 2009, the Department of Health and Human Services (HHS) is looking to impose greater financial penalties on practices that fail to comply with HIPAA rules. Since 2009, the financial penalties typically occurred with practices that over 500 records breached, but for the first time since the enforcement rules were enacted, a penalty was levied against a health care provider who breached less than 500 records. This is unprecedented and HHS has made it very clear that they will be going to use money recouped through breach-related fines to help fund ongoing enforcement. Leon Rodriguez, Director of HHS, stated, “We’re going to use as much of the money as we can to increase our enforcement capacity, especially...to move us from a complaint-driven enforcement environment to more of an affirmative enforcement environment.”

To avoid a financial penalty for a health care breach, here are five steps you should take to ensure your practice is compliant with HIPAA rules.

1. **Conduct a risk assessment of your practice.** Assign a Security Officer to oversee a risk analysis to identify potential risks and vulnerabilities. Areas to focus on include physical access to your facility, administrative access to protected health information, and protection of electronically stored data.
2. **Have documented HIPAA policies and procedures in place.** Your practice must have documented policies and procedures in place to safeguard the storage, access, and protection of health care information. Have you created a Notice of Privacy Practices, and posted it in a conspicuous location within your practice? Do you have a contingency plan in the event of a disaster such as fire, flood, or theft?
3. **Conduct employee training programs on HIPAA.** All employees should be aware of the HIPAA and HITECH rules, and employees who have access or exposure to PHI must be trained on how to protect it. They should know what constitutes PHI, when it can be disclosed, and to whom. Ongoing training is required for compliance with HIPAA rules.

4. **Have employee disciplinary policies in place.** Your practice should have written sanctions in place for failure to comply with rules regarding protected patient information.
5. **Evaluate your administrative, physical, and technical safeguards.** You should have procedures in place to safeguard the facility and equipment from unauthorized physical access, tampering, and theft. Examples include locked doors, restricting areas, and limiting access to patient information to only those employees with a need to know.

While the above list is far from inclusive in the measures you need to take to be compliant with HIPAA rules, failure to have these measures in place could result in fines and open your practice up to further liability.

About the Author

Todd McDonagh is the Chief Operating Officer at MedSafe/Total Compliance Solutions, a healthcare compliance company. Working for MedSafe brings Todd back to his roots in the healthcare industry. He started his career as a Nursing Home Administrator for Sun Healthcare Group. Before coming full circle, he was the Managing Director at The Mad Dog Group, a boutique Internet marketing and social media consultancy and the Vice President of Operations for HomePortfolio, Inc, an online product library for the home design industry. He is an Adjunct Professor of Management at the Girard School of Business at Merrimack. He has his MBA in Healthcare Management from the University of Connecticut.