Corporate compliance with federal and state laws is a must, not an option, in a well-managed medical practice. Here are eight practical suggestions for developing a compliance program that meets industry standards.

1. Be Proactive, not Reactive
The purpose of a corporate compliance program is to prevent violation of federal and state laws. A comprehensive program is both a good strategy for avoiding problems and a good defense against complaints and possible external investigation. Make sure your compliance program positions you well and is not something you address in a hurry when a problem arises.

2. Understand Scope and Organize Program Appropriately
Corporate compliance means different things to different practices. Some practices limit corporate compliance to the risk areas identified by the Office of Inspector General (OIG). We prefer a broader definition. Our list includes: coding and billing, the provision of reasonable and necessary services, appropriate documentation of care in the medical record, completion of the CMS-1500 form, attention to improper inducements/kickbacks/self referrals, retention of medical and business records, Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security, Occupational Safety and Health Administration (OSHA) and Clinical Laboratory Improvement (CLIA), if relevant.

Depending on a practice’s definition of corporate compliance, both organization and delegation of responsibility vary. Some practices centralize all compliance programs under a corporate compliance officer. In other practice settings, there is no such position and responsibility and accountability are vague. We think it makes sense to start by centralizing responsibility for corporate compliance, then delegating responsibilities appropriately. For example, in many practices, the practice manager is the corporate compliance officer. He/she may retain responsibility for HIPAA Privacy and Security and delegate responsibilities for OSHA, CLIA and coding/billing compliance to members of the clinical and billing staffs.

3. Obtain Commitment and Support from Very Top
Compliance with external legal requirements only works if the entire practice is on the same page. Make sure the owners understand the importance and scope of corporate compliance.

Not long ago the practice administrator of a large practice in North Carolina requested our help with HIPAA compliance. An out-of-state management company had responsibility for HIPAA but had not provided adequate support. The administrator knew that her practice was placing itself at great risk. Having previously worked for a large health care system that had compliance and risk management departments, she herself had never directed a compliance effort. During the course of the project, the practice accomplished a great deal, but the administrator hit the proverbial stonewall.

The practice owners refused to take the steps necessary to protect the visibility of computer screens with patient-specific information. They refused to require the use of secure user names and passwords to view a computer screen. Everyone who walked down a major corridor could easily see protected health information (PHI) by looking to the right. In addition, one particularly resistant owner prided himself on the huge piles of paper medical records he kept on a desk in a room that was visible and accessible to all. The practice administrator could only do so much because everyone wasn’t on the same page.

4. Know the Relevant Federal and State Laws
One of the most important aspects of corporate compliance is the understanding of federal and state laws that impact the running of a medical practice. At the federal level, the most important statutes are the False Claims Act (FCA), the Civil Monetary Penalties Act, the Stark Self-Referral Prohibitions, the Anti-Kickback Act of 1986, HIPAA, OSHA, and CLIA.
the location of the practice different state statutes apply.

It’s critical not only to know which laws apply, but also to remain up-to-date on changes. HIPAA is a good example. The law was passed in 1996. Although many of the provisions of the original Privacy and Security Rules have remained intact, both the 2009 Affordable Care Act and the 2013 Omnibus Final Rule made important changes. The definition of a breach has changed, and now Business Associates and Agents (i.e. subcontractors) as well as covered entities are liable.

5. Start with a Risk Analysis – and Keep Using It
A good place to start is with a risk analysis, also called a gap analysis. For each aspect of compliance, compare current with required status. Note both accomplishments and gaps, using the gaps as the launching point for developing a written plan for corrective action that specifies responsibilities and deadlines. Professional organizations, such as Medical Group Management Association (MGMA), specialty societies, the state medical society or a reliable consultant are good resources for a comprehensive list of questions.

Revisit the risk analysis every year, noting what you’ve done and identifying places where corrective action needs to be taken.

6. Develop Written Policies and Procedures
Documentation is critical. For each aspect of corporate compliance, develop written policies and procedures. Specify the purpose, responsibility, accountability, procedures, monitoring and enforcement. Date the creation/revision of the policy and procedures and review it regularly to make sure it remains compliant with external requirements and internal operations.

7. Train the Workforce
Once the Corporate Compliance Program is in place, make sure every workforce member understands the components. Create a structured training program and repeat it annually. Incorporate compliance into the orientation for all workforce members, including clinicians. In between formal training sessions, encourage workforce members to collaboratively discuss issues and concerns without fear of penalty. Make compliance an ongoing process, not a once-a-year event.

8. Marry Corporate Compliance with Human Resources
Make corporate compliance an integral part of the practice’s human resources program. Include corporate compliance requirements in job descriptions and disciplinary procedures, reminding each workforce member of the obligation to support a culture of compliance as well as to meet job expectations.

“He wanted his confidence back”
I REFERRED HIM TO SOUTHERN DERMATOLOGY