A New Year's Resolution: Updating Your Compliance Plan

By Matthew Kroplin & Kelli Fleming January 2019

Reprinted with Permission from the ***Nashville Medical News***

As January gets underway, it is common for us to reflect back on the prior year and set goals for the upcoming year. Whether it is losing weight or maintaining better relationships with loved ones, New Year's resolutions are on everyone's minds this time of year. Health care providers should also consider setting a New Year's resolution: updating your compliance plans. To be effective and beneficial, compliance policies and procedures should periodically be revised and updated, and the beginning of the year is as good a time as any to undertake such revision. Among the key compliance policies and procedures that you may want to consider updating are your corporate compliance plan, your HIPAA privacy and security plan, and your business associate agreements.

Compliance plans are written strategies, adopted by a healthcare provider, to assist in its day-to-day compliance with applicable laws and business policies. A compliance plan that is drafted without further review, revision, or implementation, however, carries the same effect as having no compliance plan at all. Thus, to be effective and beneficial, all compliance plans should be periodically reviewed and revised to address changes in the law, operational changes, and past experiences.

As you revise your corporate compliance plan, or implement one for the first time, keep in mind that among other things, the plan should include a review of the applicable laws and regulations (*e.g.*, Stark, Anti-Kickback, False Claims Act, Civil Monetary Penalties, etc.), what is expected in terms of complying with such laws and regulations, the consequences of noncompliance, and ways to report non-compliance to the appointed compliance officer or compliance committee. Policies should be written in a manner that is easy for the employee and contractor to understand.

Compliance plans should address the risks that are associated with a particular provider, contain monitoring and auditing systems that detect compliance violations, and discuss ways to address such violations. Compliance plans should include a training component, pursuant to which employees and contractors are periodically educated and trained on the elements of the plan. Training should occur both when an employee or contractor is hired and periodically thereafter (*e.g.*, every year or every six months). The compliance plan should be made available to all employees and contractors to which it applies, and should be formally adopted by the Board of Directors or similar governing body.

Similarly, based on changes in the law and increased enforcement activities, having an up-to-date HIPAA plan is extremely important. As you revise your HIPAA policies and procedures, make sure that your employees are adequately informed of your commitment to following the HIPAA plan and are properly trained regarding the HIPAA policies and procedures. If there have been any changes in applicable privacy and security laws since the last revision of your HIPAA plan, revise your plan accordingly. Also review whether your Privacy Officer and/or Security Officer is still the appropriate person(s) for the job.

On a related note, Business Associate Agreements (BAAs) are a necessary tool for ensuring HIPAA compliance, but healthcare providers oftentimes overlook this area of compliance. However, given the recent focus on business associate relationships by the Office of Civil Rights, the government agency overseeing HIPAA

compliance, healthcare providers should not only ensure that a BAA is in place when one is necessary, but also that the BAA reflects the intentions of the parties.

BAAs contain numerous provisions that may require review and negotiation, but our top several provisions to look for when reviewing a BAA include: indemnity provision; breach reporting; timely access to patient information (or related accounting information) to help facilitate a patient's request for access, request for amendment, or request for an accounting in accordance with HIPAA; de-identification of data; and choice of law.

Although you may waiver on your other New Year's resolutions (we assure you that ours will be broken before the end of the month!), updating your compliance policies and procedures, especially your corporate compliance plan, your HIPAA policies, and your BAAs, is one resolution that should be, and can be, kept.

For more information, please contact:

Matthew Kroplin
Partner, Nashville Office
P. (615) 724-3248
E. mkroplin@burr.com

Matthew Kroplin is a partner in Burr & Forman's Nashville office, practicing in the firm's health care and business litigation sections.

Kelli Carpenter Fleming
Partner, Birmingham Office
P. (205) 458-5429
E. kfleming@burr.com

Kelli Fleming is a partner in Burr & Forman's Birmingham office, practicing exclusively within the firm's health care section.