The Quest for HIPAA Compliance: What Could Go Wrong?

Michael J. Murray

October 2014

With enough prodding any HIPAA lawyer will tell you the truth about HIPAA compliance: most of the healthcare industry is still playing catch-up. Very few organizations are in strict compliance with HIPAA, even those who have allocated meaningful staff time and resources into getting up to speed. In my experience, the HIPAA blind spot persists for a couple of reasons. First and foremost, HIPAA is overly complicated, comprising more than 100 pages of fine-print rules and procedures that would test the will of the most persistent of compliance managers. The truth is, HIPAA compliance is not easy and requires a substantial and on-going investment of staff time and legal guidance.

Second, HIPAA compliance falls under the same category as speeding and being honest on your taxes. If the government isn't always looking, partial compliance is good enough, isn't it? From a lawyer's perspective, that is never the right answer and the assumption that enforcement is lacking is no longer true. In 2013, Health and Human Services (HHS) nearly doubled the number of completed HIPAA investigations over the prior year, up to almost 10,000 in 2013 alone. And to bring home this point, when HHS does impose a penalty, the figures tend to be high. Two of the fines levied in the first half of 2014 were over $4 million. So what can a health organization do to become HIPAA proof?

Here are seven essential steps:

1 The Risk Analysis

This is the heavy-lift when it comes to developing a meaningful HIPAA program. Organizational leaders must sit-down together, often for several hours and in several sessions, to determine where threats to protected health information exist in the organization's practices, procedures, and personnel and, importantly, how to address those threats. If you haven't drilled down into how health information can escape from your practice on a day-to-day, encounter-to-encounter basis, then you have not conquered HIPAA.

2 Putting it on Paper

Once you've completed your Risk Analysis, you have to memorialize your work into comprehensive policies and procedures. These documents will direct your administration and staff on how to safeguard protected health information at your organization.

3 Putting the World on Notice

These policies and procedures must also be written up into a Notice of Privacy Practices that advises all patients and clients on exactly how their health information will be handled in your office. The Notice must be given to every patient or client at the first treatment encounter and must be posted on the organization website.

4 Business Associate Agreements

All business partners and service professionals who receive or create protected health information on behalf of your organization must sign an adequate Business Associates Agreement. This ensures that the sensitive information entrusted to your business partners and vendors is also protected by HIPAA since many of these companies are not HIPAA covered entities.

5 Review Authorization Forms

To be valid under HIPAA and state laws, authorization forms must contain several required warnings and meet other stringent factors, the absence of which will invalidate the authorization. These forms are used over and over again by your staff in order to give or gain access to highly sensitive information so make sure yours are up-to-date and legally sound.

> "Two of the fines levied in the first half of 2014 were over **$4 million.**"

6 The Critical Step – Training

After expending all of that energy developing and writing down your policies and procedures, make sure you don't skip the final vital step: training your staff. To reduce your chances of a HIPAA violation, your staff must be educated on how to properly safeguard patient information when it comes to daily practice, use of technology, interactions with vendors and effective mitigation steps when an information breach does occur. All of your hard work is for naught if you don't impart your HIPAA compliance plans with your staff. Plus, the HIPAA rules require it.

7 Vigilance is Required

If the last time your organization conducted a HIPAA tune-up was "a couple of years ago" you are likely woefully out of compliance. HIPAA requirements change often (important updates occurred in September 2013). Moreover, policies and training must be updated as your internal practices and technology tools change. Revisit your HIPAA program regularly and do not let your guard down.

If you have any questions about any of the topics discussed in this advisory, please contact your Drummond Woodsum attorney.

Michael J. Murray
207.253.0547
mmurray@dwmlaw.com

Michael J. Murray is a lawyer with Drummond Woodsum with a specialty in HIPAA compliance. He is a graduate of Stanford Law School.