Taking the Necessary Steps
An Interview with a HIPAA-Compliant Practitioner

Dr. Charlie Cooper of Chapel Hill, NC, heads up a multidisciplinary group practice consisting of 28 providers in two cities. His practice is compliant with both Privacy and Security regulations of the Health Insurance Portability and Accountability Act (HIPAA). Because the process he went through can work for psychologists in a wide range of practices, Good Practice (GP) asked him about what it takes—and why it’s important—to become HIPAA compliant.

Privacy Rule Compliance

GP: What steps have you taken to become compliant with the HIPAA Privacy Rule?

Dr. Cooper: So much of HIPAA compliance depends on context. How one implements the Privacy Rule is conditioned on the size and complexity of one’s practice or institution. Here are some of the steps we took in our practice:

1. We appointed a Privacy Officer (me).
2. We studied the Privacy Rule to understand what we needed to do to become compliant.
3. We prepared Policy and Procedures for the practice.
4. We created a Notice of Privacy Practices to distribute to our patients.
5. We trained clinical and support staff in our policies and procedures.
6. We had contractors who work with our practice sign Business Associate Agreements.

GP: Where did you find the resources you needed?

Dr. Cooper: We looked around for resources and selected the Privacy Rule product that was created by the APA Practice Organization. It provided state-specific templates for all the essential documents we used to articulate policies, inform patients, set up contracts with business associates and record the relevant data that must be maintained in order to demonstrate compliance. The four hours of continuing education credit were an added bonus.

GP: How long did it take to put your Privacy Rule process in place?

Dr. Cooper: In our practice, the process required between 15 and 25 hours of my time as the privacy officer, including

(continued on page 2)
Dear Practitioner:

This newsletter is the first in a planned series of topical editions of *Good Practice* that supplement our annual magazine. This issue of *Good Practice* from the APA Practice Organization focuses on HIPAA compliance and contains information of particular interest to our members.

The federal Health Insurance Portability and Accountability Act (HIPAA) is intended as a major step toward making our health care system more efficient through the use of information technology. But the voluminous rules resulting from this act—the Privacy and Security Rules in particular—have added to the complexity of practice.

Both of these rules are equally important for practitioners, and each requires a separate set of compliance activities. Practitioners have turned to us for guidance to help ensure that they implement HIPAA fully and appropriately.

In this issue, one of our peers describes the steps he took to make his practice compliant with the HIPAA Privacy and Security Rules. You’ll also learn how these two HIPAA rules differ, how psychotherapy notes are afforded heightened privacy protection under HIPAA, how to apply for your National Provider Identifier (NPI), potential penalties for non-compliance with HIPAA, and more.

We at the Practice Organization remain committed to serving you in numerous ways through this and other resources. We hope you’ll keep this newsletter handy and share it with colleagues.

The APA Practice Organization is constantly seeking ways to help members with the challenges and opportunities of practice in the current health care delivery system. As always, we invite your comments and suggestions. Please feel free to call us toll-free at 800-374-2723 or send your email to practice@apa.org.

Sincerely,

Russ Newman. PhD, JD
Executive Director for Professional Practice

P.S. Look for the next issue of *Good Practice* magazine in the spring of 2007.

**Questions About HIPAA?**

Staff for the APA Practice Organization are available to help members with questions about HIPAA. Contact us toll-free at 800-374-2723 or send an email to practice@apa.org.

---

**Taking the Necessary Steps**

(continued from page 1)

**Security Rule**

GP: What steps did you take to become compliant with the HIPAA Security Rule?

Dr. Cooper: Our efforts toward Security Rule compliance included the following:

1. We designated a Security Officer (again, that honor fell to me).
2. We conducted a risk analysis, identifying risks we needed to abate through administrative, physical and technical measures.
3. Following the risk analysis, we prepared the required documentation of our compliance policies and procedures.

GP: What resources helped you create the documentation necessary for compliance?

Dr. Cooper: We utilized the online compliance workbook from the APA Practice Organization. As with the Privacy Rule resource, the workbook provided templates that simultaneously walked us through a risk analysis and, for each standard and implementation specification, suggested language we could use—and action steps we could take—to address potential risks.

GP: How long did it take you to complete both the risk assessment of your practice and the compliance documentation?

Dr. Cooper: It took 10 to 12 hours. However, I would estimate for a solo or a two- to four-person practice, the time requirement would be far shorter because the compliance process would be less complex due to things such as fewer employees and practice locations.

---
Which actual Security Rule compliance activities did you implement in your practice?

Dr. Cooper: Interestingly, we found that most implementation standards were already being met within our practice. For example, we had already installed computers with password-protected access controls and thorough backup procedures. We had firewalls and antivirus protection. We had taken physical measures to assure that protected health information was secured in locked areas. And we already had begun to outline disaster-recovery procedures.

So in our case, the bulk of activities necessary for compliance were focused on documentation and training. As a result, for our practice, becoming compliant involved conducting a formal risk assessment, documenting our solutions to identified risks, creating all necessary policies and procedures and, finally, giving an orientation and training for staff. We had a computer consultant on retainer, so we had him sign a Business Associate Agreement.

After studying the Security Rule, our computer consultant told us, “The good news is that HIPAA’s requirements are largely measures that any business should take to protect data in the first place.”

GP: Do you have any recommendations for psychologists who feel they may need assistance understanding the technical issues involved in the Security Rule?

Dr. Cooper: My nearly blanket recommendation for anyone attempting to comply with the Security Rule is to form a reliable relationship with an information technology expert who can provide assistance in an emergency and is willing to sign the Business Associate Agreement so he or she can work on your computers, PDAs, etc., as needed.

Compliance Issues

GP: What were your biggest challenges in becoming HIPAA compliant, and how did you address them?

Dr. Cooper: The biggest challenge was drafting, updating and maintaining the documentation required by each rule. We dealt with the initial documentation process almost exclusively by using the templates included in the APA Practice Organization’s online products. The long-term challenge will be to update our documents, especially those pertaining to the Security Rule. Because while the Privacy Rule compliance steps remain largely unchanged, Security Rule implementation is continually subject to change as technology renders past solutions obsolete. It has proved difficult, even in a large practice like ours, to exert the oversight and discipline to document all the evolutionary changes that occur—usually technology-driven—such as when we acquire and install new software.

GP: Is it really that important to be HIPAA compliant?

Dr. Cooper: Yes, and there are many reasons for investing in HIPAA compliance. Perhaps most important, in an increasingly technologically sophisticated era, HIPAA rules can be highly protective of our clients. I can give you one example: I had a palm device that contained a small amount of unencoded, client-specific information on it. Neglectfully, I left it behind in a store where I was shopping. While I discovered the loss within five minutes and recovered the PDA immediately, the lesson was pounded in and has stuck indelibly. Now my PDA has automatic data encoding and fingerprint recognition as a password.

Additional reasons for compliance include the fact that many privacy and security decisions often surface suddenly, as when sensitive records are requested or when there is a security breach. To attempt compliance after the horse has jumped the fence could jeopardize not only patients but also one’s practice standing with licensing authorities or in litigation. HIPAA is getting so well-known that it surely will be the basis for legal actions in the future. In my view, it’s important to be HIPAA compliant even for practices that do not transmit electronically, and

(continued on page 7)
8. Referral Certification and Authorization
Communications including: a request for the review of health care to obtain an authorization for the health care, a request to obtain authorization for referring an individual to another health care provider, or a response to one of these requests.

The following two transactions have yet to be formally defined by the Department of Health and Human Services, so we have provided a basic definition below.

Communication where an injury is reported to the worker’s compensation carrier for any potential workers compensation claim.

10. Health Claims Attachments
An extraction of relevant information from the medical record to demonstrate the reason for the service provided and the subsequent health care claim.

Once a psychologist—or an entity such as a billing service acting on behalf of the psychologist—triggers HIPAA, the Privacy Rule applies to all protected health information in the psychologist’s practice. Once HIPAA is triggered, the Security Rule applies to all electronic protected health information in a practice.

thus have not “triggered” HIPAA. This is because compliance with the Privacy Rule assures sound treatment of confidential information and clear communication with clients regarding that information. Compliance with the Security Rule is consistent with good business-information practices. And it is increasingly easy to trigger that rule inadvertently through an emergency action such as transmission of an email or computer-based fax.

GP: What are the biggest misconceptions practitioners may have about HIPAA compliance?

Dr. Cooper: From my experience fielding calls regarding HIPAA issues as Director of Professional Affairs in the North Carolina Psychological Association, the biggest misconception among practitioners may be that HIPAA is largely irrelevant to practice. It often may seem true—until the moment it becomes not only relevant but indispensable in resolving some unforeseen privacy or security issue.

Another common misconception is that many practitioners think if they’re compliant with the Privacy Rule they’ve satisfied all of their HIPAA obligations, which is absolutely not true.

GP: Is it important to comply with both the Privacy and Security Rules?

Dr. Cooper: Yes, because they’re synergistic: you can’t fully implement one without the other. Without the Privacy Rule, you don’t know what to protect. Without the Security Rule, you don’t know if you have “holes” in the protective shield.

GP: What advice would you give to other practitioners about becoming HIPAA compliant?

Obtain the tools for each rule, designate several blocks of time and persevere. With the confidence the Practice Organization’s tools provide, the process is not only achievable, it can actually become interesting.

Once you’re compliant, it’s also important to be aware that if aspects of your practice change, such as hiring a new staff person, you may need to revisit and update your policies and procedures to ensure ongoing compliance.

GP: Is there any other advice you can give to practitioners who have not yet taken steps to become HIPAA compliant?

If you did not meet the deadline for HIPAA compliance, you still should implement. It’s an important aspect of risk management for your practice, and compliance can definitely be accomplished in small steps.

The HIPAA compliance information and resources mentioned in this article can be found on APApractice.org. See page 20 for a list of additional resources for help with HIPAA.

1 Under HIPAA, “protected health information,” or PHI, is information that: is transmitted or maintained in any form or medium; relates to the past, present or future: physical or mental health condition of an individual; the provision of health care to an individual; or payment for providing health care to an individual; and identifies the individual or could reasonably be used to identify the individual. For psychologists, this generally means information about a specific patient, client or person you are evaluating.

2 Electronic protected health information, or EPHI, is PHI that is transmitted or stored in electronic form.