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)
T his newsletter is the first in a planned series of topical editions of Good Practice from the APA Practice Organization that supplement our annual magazine. This issue 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. We hope you’ll keep this newsletter handy and share it with colleagues.

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 about 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.

Dear Practitioner:

With the HIPAA Privacy and Security Rules. You’ll also learn about 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.

Dr. Charlie Cooper

This newsletter contains information about HIPAA compliance of particular interest to practicing psychologists. Learn more at APApractice.org.

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.

Introducing a New Resource
A Focus on HIPAA Compliance

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 breach. To attempt compliance after the horse has jumped the fence could jeopardize not only patients ... in the future. In my view, it’s important to be HIPAA compliant even for practices that do not transmit electronically, and...
Six Reasons Why HIPAA Matters

Have you ever wondered if HIPAA compliance is really vital to you as a practicing psychologist? If there’s ever been a doubt in your mind, the following considerations may help you reconsider the matter.

1. Compliance is a matter of law.

The most obvious consideration is if you as a health care practitioner take actions that trigger HIPAA, you must comply fully with the HIPAA rules. This includes all health care professionals who electronically transmit health information in connection with standard transactions designated under HIPAA. (See “What Triggers the Need to Comply?” on page 6 for a list of the standard transactions that trigger HIPAA.) There are substantial penalties associated with failure to comply with HIPAA. (See the article, “Final HIPAA Enforcement Rule Takes Effect,” page 16).

The following considerations apply even if a psychologist does not technically trigger HIPAA.

2. The health services delivery industry is fast moving toward electronic transactions.

Increasingly, participation in health insurance programs requires electronic claims submission and other electronic transactions that trigger the need for HIPAA compliance. Payers are creating incentives for such participation, for example, by reimbursing more quickly for claims submitted electronically than for paper claims. Even health professionals who do not yet engage in electronic transactions can ensure that their future actions do not put them in violation of HIPAA by complying now. For example, should they decide at some point to employ an electronic billing service or to take a client whose health insurance plan requires electronic billing, these practitioners will have no “grace period” for meeting HIPAA requirements. Full compliance will be required beginning at the moment electronic billing is initiated.

3. HIPAA helps protect your patients.

The Privacy and Security Rules entail requirements that help protect the privacy and confidentiality of the therapist-client relationship. These should be matters of central concern to mental health professionals. Following the Privacy and Security Rules—for example, by keeping HIPAA-compliant psychotherapy notes (see “Practitioners: Take Note,” page 8) and by using safe email practices—can protect client confidences from insurance companies as well as computer hackers.

4. HIPAA requirements constitute sound business practice.

Consider the example of “contingency planning” as required by the HIPAA Security Rule. Taking steps to ensure that electronic protected health information (EHI) can be recovered and restored in the event of an emergency can lessen interruptions to your practice. For example, there were practitioners affected by Hurricane Katrina who needed to recover lost electronic patient data.

Those who had backed up and stored their patient records in a location safe from flooding, consistent with the HIPAA Security Rule, were prepared to recover what they needed. Taking this important step in advance helped minimize disruptions to continuity of patient care. Others who lacked backup files were not as fortunate.

Following HIPAA specifications can help you avoid potential risks.

As one example, the Security Rule requires practitioners to implement policies and procedures to address the final destruction and/or disposal of EHI and computers or other devices in which EHI is stored. Disposing of a computer without using software that completely removes patient records is contrary to HIPAA requirements. There are reports of computer programs being used to recreate patient files that a psychologist thought he or she had “deleted.” The use of such programs may jeopardize confidential patient health information and increase the psychologist’s risk of liability.

The Privacy and Security Rules are likely to be invoked as setting the standard of care in the health care industry. Many health care analysts have advanced this argument. HIPAA requirements could be brought to bear in legal and professional disciplinary deliberations, even in situations where HIPAA compliance technically has not been triggered.

There are reports of computer programs being used to recreate patient files that a psychologist thought he or she had “deleted.” The use of such programs may jeopardize confidential patient health information and increase the psychologist’s risk of liability.

6. The Privacy and Security Rules are likely to be invoked as setting the standard of care in the health care industry.

There are reports of computer programs being used to recreate patient files that a psychologist thought he or she had “deleted.” The use of such programs may jeopardize confidential patient health information and increase the psychologist’s risk of liability.
What Triggers the Need to Comply?

Both the HIPAA Privacy Rule and Security Rules are triggered when a psychologist, or an entity such as a billing service acting on behalf of the psychologist, transmits electronic protected health information in connection with any designated standard transactions (items 1 through 10 at right).

Transmission in “electronic form” includes transmission via the Internet, extranets (using Internet technology to link a business with information only accessible to collaborating parties), leased lines, dial-up lines, computer-generated faxes (not traditional paper-to-paper faxes), private networks and electronic protected health information (EPHI—see footnote 2, page 7) that is physically moved from one location to another using magnetic tape, disk or compact disk media.

Following are the standard transactions. For psychologists, the transactions most likely to trigger HIPAA are communications from the practitioner related to insurance claims or eligibility (items 1, 3, 4, 5, 6 and 8). The definitions that appear below are summaries of the definitions provided by the U.S. Department of Health and Human Services in 45 C.F.R. Sections 62.1101-162.1802.

1. Health Care Claims
Requests to obtain payment and the necessary accompanying information from a health care provider to a health plan, for health care services rendered.

2. Health Care Payment and Remittance Advice
Payment information about the transfer of funds or payment processing information from a health plan to a health care provider’s financial institution, or either the explanation of benefits or remittance advice from a health plan to a health care provider.

3. Coordination of Benefits
Inquiries from any entity to a health plan for the purpose of determining the relative payment responsibilities of the health plan regarding either claims or payment information (e.g., whether payment should be made instead by another insurer, Medicaid, etc.).

4. Enrollment or Disenrollment in a Health Plan
Inquiries regarding subscriber enrollment information provided to a health plan to establish or terminate insurance coverage.

5. Health Care Claim Status
Inquiries used to determine the status of a health care claim or a response about the status of a health care claim.

6. Eligibility for a Health Plan
Either: (1) an inquiry from a health care provider to a health plan or from one health plan to another health plan to obtain information about a benefit plan for an enrollee regarding eligibility to receive health care under the plan, coverage of health care under the plan, benefits association with the plan, or (2) a response from a health care plan to the provider or other health care plan regarding the same.

7. Health Plan Premium Payments
The communication of other payment information about the transfer of funds, detailed remittance information about individuals for whom premium payments are being paid, or payment processing information such as payroll deductions, associated group premium payment information or other group premium payments.

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.

Taking the Necessary Steps (continued from page 6)

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 seems 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: What advice would you give to other 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.
Practitioners: Take Note  HIPAA provides extra privacy protection for psychotherapy notes

Typically, these “excluded” items comprise the other part of the patient record (often referred to as the clinical record) that is separate from psychotherapy notes.

**Patient authorization required to release psychotherapy notes**

The Privacy Rule requires psychologists and other entities covered under HIPAA to obtain specific patient authorization for the disclosure and use of “psychotherapy notes.” Under HIPAA, disclosing psychotherapy notes to others calls for more than just notice or general consent. Explicit patient authorization—written permission from the client that meets specific Privacy Rule requirements—is needed to release psychotherapy notes to, or let them be viewed by, anyone other than the therapist who created them.

This authorization requirement applies to records requests from managed care and other health plans. It even protects clients from having other mental health professionals in the same group practice view the psychotherapy notes unless the client has authorized it.

**Insurance companies barred from access to psychotherapy notes**

Before the HIPAA Privacy Rule took effect, insurance companies sometimes requested entire patient records, including what are now called psychotherapy notes, in making “medical necessity” decisions. Patients could decline to have this type of information released, but the insurance company might deny coverage for related services.

Now health plans cannot refuse to provide or authorize reimbursement to the patient or psychologist if a patient does not agree to release psychotherapy notes. The HIPAA Privacy Rule forbids such refusal to pay. Further, managed care companies may not require you to turn over psychotherapy notes during an audit of your patient records. Even so, insurers can refuse to pay for services if medical necessity is not sufficiently documented in the clinical record. So it is advisable for the clinical record to provide adequate rationale for medical necessity.

**Patient access to information in the client record**

The HIPAA Privacy Rule also generally protects psychotherapy notes from being viewed by the patient. However, because this federal regulation does not preempt state laws that give patients greater access to their records than HIPAA does, patient access to psychotherapy notes varies from state to state.

In some states, the Privacy Rule prevails and the patient has no right to access psychotherapy notes. In other states, the psychologist has greater discretion to withhold psychotherapy notes than to withhold the clinical record. In a third group of states, psychotherapy notes have no greater protection from patient access than the clinical record.

**Keeping “separate” psychotherapy notes**

The HIPAA definition of “psychotherapy notes” explicitly states that these notes must be kept “separate” from the rest of the patient record, but does not specify what “separate” means. It seems clear, however, that if the psychologist maintains the notes in a general chart along with other clinical information, the notes would not qualify for the heightened privacy protection that HIPAA provides for psychotherapy notes.

In light of the HIPAA rule wording, practitioners should consider whether someone else would be able to readily “distinguish” their psychotherapy notes from the rest of the record. If another person could do so, the psychotherapy notes likely would be considered as separate from the clinical record. As one approach, psychologists separate their psychotherapy notes by keeping them on one side of the patient’s file folder, while putting the clinical record on other side.

When keeping separate records electronically, the psychotherapy notes should be located in a separate electronic file, or separate part of the electronic file, and preferably labeled as “confidential” and/or “psychotherapy notes.” In addition, they should have a higher level of security, such that only the therapist who created them has access (unless the patient has authorized broader access). Keep in mind that maintenance of electronic records also raises important issues related to HIPAA Security Rule compliance.

**Why “psychotherapy notes” are offered special privacy protection**

During the rule-making process, APA successfully advocated to the U.S. Department of Health and Human Services (HHS) that the final Privacy Rule should provide heightened protection for psychotherapy notes. In doing so, the Privacy Rule recognizes that the kinds of information contained in psychotherapy notes need a higher level of privacy protection than other types of information kept in patient records.

HHS accepted APA’s arguments that psychotherapy notes reflect communications whose confidentiality is essential to successful psychotherapy and that these notes serve as the therapist’s private notes for his or her own use. As such, they are not needed by or to be shared with others in the health care delivery system such as third party payers and other health care professionals.

1 State-specific patient authorization forms as well as state-by-state information about patient access to psychotherapy notes is part of HIPAA for Psychologists, the online Privacy Rule compliance tool from the APA Practice Organization designed for practicing psychologists. Visit the “HIPAA Compliance” and “AFCpractice.org Store” sections of AFCpractice.org for details and ordering information.

(continued on page 12)
The HIPAA Privacy and Security Rules: A Side-by-Side Comparison

Some health care professionals have mistakenly believed that, by complying with the requirements of the HIPAA Privacy Rule, they have met most or all of their obligations under HIPAA. Although there is a bit of overlap between the HIPAA Privacy and Security Rules, each rule is distinct and requires its own compliance process.

A fundamental distinction is that the Privacy Rule focuses on intentional releases of protected health information, while the Security Rule focuses on safeguarding your practice against unintentional disclosures. Another difference is that the Privacy Rule calls for a thorough comparison of the rule with your state laws related to confidentiality of patient records; the Security Rule does not require such a comparison.

The table below highlights several of the major differences and similarities in the HIPAA Privacy and Security Rules.

**HIPAA PRIVACY RULE**

- Protecting “electronic protected health information,” or EPHI, from unintended disclosure through breaches of security and from unintended loss, for example, through fire or flood.

**HIPAA SECURITY RULE**

- The same transactions as listed for the Privacy Rule.

### Focus

**HIPAA PRIVACY RULE**

- Applying policies and procedures to control when, under what circumstances and to whom to release protected health information, or PHI. The Privacy Rule focuses on intentional releases of PHI.

**HIPAA SECURITY RULE**

- Protecting “electronic protected health information,” or EPHI, from unintended disclosure through breaches of security and from unintended loss, for example, through fire or flood.

### What triggers the rule

**HIPAA PRIVACY RULE**

- The Privacy Rule is triggered when a psychologist transmits PHI in electronic form in connection with any of the following types of transactions:
  - Health care claims
  - Health care payment and remittance advice
  - Coordination of benefits
  - Health care claim status
  - Enrollment or disenrollment in a health plan
  - Health claims attachments
  - Eligibility for a health plan
  - Health plan premium payments
  - Referral certification and authorization
  - First report of injury
  - Further, the Privacy Rule is triggered when an entity acting on behalf of the psychologist, such as a billing service, transmits PHI in electronic form.

**HIPAA SECURITY RULE**

- The same transactions as listed for the Privacy Rule.

### What the rule applies to

**HIPAA PRIVACY RULE**

- Once a psychologist triggers HIPAA, the Privacy Rule applies to all PHI in the psychologist’s practice.

**HIPAA SECURITY RULE**

- Once a psychologist triggers HIPAA, the Security Rule applies to all EPHI in a psychologist’s practice.

### Major steps toward compliance

**HIPAA PRIVACY RULE**

- Determine what state laws related to privacy are more stringent than the Privacy Rule.
- Develop a notice of privacy practices and authorization form (shaped by the interaction of state privacy laws and the Privacy Rule), as well as a Business Associates Contract and other forms you may need for compliance.
- Designate a “Privacy Officer” responsible for ensuring that appropriate privacy procedures are adopted and followed (also see section below on “Scalability”).
- Document and implement policies and procedures in light of the rule’s requirements, for example, a patient complaint process.
- Train employees to carry out their functions under the Privacy Rule.

**HIPAA SECURITY RULE**

- Conduct a formal risk analysis of your practice. The risk analysis is a thorough assessment of the practice’s potential security risks and vulnerabilities related to EPHI.
- Designate a “Security officer” responsible for ensuring that appropriate privacy procedures are adopted and followed. In a solo practice, this will be the individual psychologist. In a small or large group practice, one of the psychologists or office staff can be designated as the Security Officer.
- Implement safeguards to minimize any risks you have identified.
- Develop security policies and procedures in light of your risk analysis and the safeguards you have chosen.
- Document measures that the practice has taken to comply with the Security Rule.

### Scalability

**HIPAA PRIVACY RULE**

- The administrative requirements of the Privacy Rule are “scalable,” meaning that a health professional covered by HIPAA must take “reasonable” steps to meet the requirements according to the size of practice and type of activities. A key example: while a hospital might be required to create a full-time staff position to serve as a Privacy Officer, a psychologist in solo practice may identify himself or herself as the Privacy Officer.

**HIPAA SECURITY RULE**

- The same provisions as for the Privacy Rule.

### Interaction with state law

**HIPAA PRIVACY RULE**

- The HIPAA Privacy Rule establishes a minimum set of requirements for protection of PHI. The federal rule does not preempt, or override, state laws that are stricter in safeguarding an individual’s PHI or that give the patient greater access to his/her PHI. Practitioners need to determine for their particular state whether HIPAA preempts state law, or whether stricter state law applies.

**HIPAA SECURITY RULE**

- Not applicable to the Security Rule. Compliance with the rule does not vary because of state law.

### Responsibility for violations by business associates

**HIPAA PRIVACY RULE**

- HIPAA requires health professionals to enter into contracts with business associates (such as accountants, lawyers or a billing service) with whom they share PHI as defined under HIPAA. In essence, the psychologist needs to contractually obligate the business associate to follow all HIPAA compliance requirements that the psychologist must follow. Having an appropriate business associates contract protects the psychologist from liability if the business associates violate HIPAA obligations.

**HIPAA SECURITY RULE**

- Same as for the Privacy Rule.

### Table Differences and Similarities

<table>
<thead>
<tr>
<th>Privacy Rule Differences</th>
<th>Security Rule Differences</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protects PHI</td>
<td>Protects EPHI</td>
</tr>
<tr>
<td>Requires intentional releases</td>
<td>Requires safeguarding</td>
</tr>
<tr>
<td>Requires notice</td>
<td>Requires policies and procedures</td>
</tr>
<tr>
<td>Requires privacy</td>
<td>Requires security</td>
</tr>
<tr>
<td>Officer required</td>
<td>Officer optional</td>
</tr>
<tr>
<td>State law preemption</td>
<td>State law not applicable</td>
</tr>
<tr>
<td>Specific requirements</td>
<td>Specific requirements</td>
</tr>
</tbody>
</table>

---

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, 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.

3. For additional information, see “What Triggers the Need to Comply?” on page 8.

4. HIPAA online compliance is provided by or under the business associates contract to psychologists that may be customized. Visit the HIPAAonline.org home page or HIPAAonline.org for additional information.
Kinds of information included in psychotherapy notes in line with HIPAA

Psychotherapy notes are designed to protect information whose sanctity is important to maintaining the therapeutic relationship. Some practitioners reflect in these notes the patient’s intimate confidences and sensitive information about persons other than the patient, along with the psychologist’s speculations and unformed opinions.

Making decisions about what to keep, and what not to include, in psychotherapy notes may be found in the rationale embraced by HHS in finalizing the Privacy Rule—namely, that psychotherapy notes are the therapist’s private notes that are not typically used by or shared with other professionals or with third party payers.

If the information should be shared with other health professionals involved with the patient’s care, this constitutes a reason to put it in the clinical record. For example, a notation that the patient reported feeling irritable after taking a psychotropic medication would fall into this category. And if the information is among the “exclusions” to the HIPAA definition of psychotherapy notes, that information should be included in the clinical record.

Sometimes the decision about what to record where is a matter of detail, as the psychologist keeps in mind whom might ultimately have access to the information. For example, a practitioner might note in the clinical record the symptom that the patient is having night terrors. But the details of those nightmares and the psychologist’s initial musings about their significance, which are less important to other health care professionals, would go in the psychotherapy notes.

Although placing information in the psychotherapy notes always protects information from health insurers and may bar patient access, keep in mind that there are a variety of situations where outside parties may have access to psychotherapy notes. For example, a client might have to authorize their release for a military or government job application, or a court may order the disclosure of records. Accordingly, the psychologist should consider such potential disclosures when making psychotherapy note entries.

What if a practitioner does not keep separate psychotherapy notes?

Practitioners subject to HIPAA need to consider the practical effect if they choose not to keep separate psychotherapy notes. In contrast to the clear protections for psychotherapy notes, psychologists who keep their records combined have only the Privacy Rule’s vague “minimum necessary disclosure” standard to rely on when arguing that insurers and others should not see the entire record.

When “protected health information” is disclosed or used, the Privacy Rule requires psychologists to share the minimum amount of information necessary to conduct the activity. The requesting party will often argue that the entire record is the “minimum” that they need, while the psychologist counters that a much narrower set of records is appropriate to release. It is conceivable that the final arbiter of what is “minimum necessary disclosure” in a case such as this could be a court of law in the event that a legal dispute ensued.

Additional Considerations

Also be mindful of the following additional considerations related to keeping psychotherapy notes and other elements of patient records:

• Insurance company employees may not understand that HIPAA precludes them from looking at psychotherapy notes. Some practitioners report having interactions with managed care company representatives who are seemingly unaware of the HIPAA privacy protections that apply to psychotherapy notes.

• A number of other important considerations have a bearing on record keeping, including applicable state law; APA’s Record Keeping Guidelines (which are being revised); APA’s ethical principles; and institutional policies governing record keeping (for example, policies that apply to psychologists employed in a health care facility).

FIND OUT MORE

To learn more about the HIPAA rules and how to comply, visit the “HIPAA Compliance” section of APApractice.org.
Applying for Your National Provider Identifier

A Q&A for Psychologists

A s of May 23, 2007, all health care professionals will be required to have a National Provider Identifier (NPI) to use when billing electronically any government or private health insurer. The creation and use of the NPI raise a number of questions for practicing psychologists. This question-and-answer article addresses several common inquiries.

Q. What is the NPI?
A. The NPI is a unique 10-digit number assigned to every health care provider or entity that applies for it. This number will replace other provider identification numbers, such as Medicare’s Unique Physician Identifier Number (UPIN), that have been assigned to health care professionals by government and private insurers for use in billing. Once a health professional receives an NPI, that number is assigned to that health professional for his or her entire career, regardless of whether the health professional relocates, changes employers or even changes health professions.

Q. How is the NPI used?
A. The NPI is intended for use in identifying practitioners when they transmit health information electronically—for example, in submitting claims for payment and referral authorizations.

Q. Who must apply for an NPI?
A. All “covered entities” under the Health Insurance Portability and Accountability Act (HIPAA), which includes all health care professionals who are required to comply with this federal law, must obtain an NPI no later than the May 23, 2007 deadline. In essence, the need to comply with the Privacy Rule is triggered when a practitioner transmits protected health information in electronic form in connection with health care claims and other transactions as specified in the rule.

The “HIPAA Compliance” section of APApractice.org contains further information about what constitutes a “covered entity” under HIPAA. In addition, the Centers for Medicare and Medicaid Services Web site includes “tools” for determining if you’re a covered entity. The relevant Web site is http://www.cms.hhs.gov/apps/hipaacompliance/default.asp.

Any private health insurer can require that health professionals who bill the insurer use an NPI, even if the billing is done by mail rather than electronically. This means that even psychologists who are not considered “covered entities” under HIPAA likely will be required to get an NPI. Therefore, the APA Practice Organization encourages all psychologists who bill private and/or public health insurance plans, including federal and state programs, to obtain an NPI.

Q. If I am not covered under HIPAA and I apply for an NPI, will I automatically be required to comply with HIPAA?
A. No. Applying for an NPI does not “trigger” your having to comply with HIPAA.

Q. Do I apply for an NPI as an individual or organization?
A. Every individual and organization covered under HIPAA must obtain an NPI. The overarching rule is that if you have an organization that your state views as separate from the individual, the organization should obtain its own NPI. Sole proprietorships, which are unincorporated businesses, generally are not considered separate and distinct from the individual owner. For that reason, sole proprietorships should apply as individuals, using a social security number, not their employer identification number (EIN). On the other hand, corporations are usually seen as separate and distinct, so they should apply for a separate NPI apart from the individual health care professionals who work for the corporation.

A group practice (that is not a sole proprietorship) should obtain its own NPI and all the psychologists who work in that group should get their own unique NPIs. The group practice’s NPI and the individual psychologists’ NPIs are not linked in any way. This allows the individual psychologists to bill for services rendered at other places such as in a hospital or in another group practice—for example, if they work part-time in more than one setting. Further, it allows individuals to leave one group practice and join another without having to worry about changing their NPI.

Q. What will health insurers and others know about my practice based on the NPI assigned to me?
A. Unlike identifiers used by the government and health insurers in the past, the NPI is a random number. The 10-digit number does not reveal any information about the health professional, such as geographic location or type of practice. Yet, while no such information can be gleaned from the NPI itself, insurers may have access to certain information included in your NPI application, such as your choice of taxonomy code (discussed further in this article).

Q. What steps do I take to apply?
A. The steps you take depend on whether you file electronically or submit paperwork to obtain an NPI.

Electronic Application Process

Psychologists may complete and submit the NPI application form online by accessing https://nppes.cms.hhs.gov. You will be able to complete the application quickly, so long as you have all the required information ready before you begin. The list of information needed for individuals applying for an NPI includes:

- Health practitioner name
- Health practitioner date of birth
- Country of birth
- State of Birth (if birth was in the United States)
- Health practitioner gender
- Social Security Number or other proof of identity

Electronic submission is the fastest way to obtain your NPI. The Web site listed above will walk you through the steps involved in completing the application. The Center for Medicare and Medicaid Services (CMS) advises that electronic submission is the fastest way to obtain your NPI.

Paper Application Process

For any health care professional who wishes to complete a hard copy version of the application form and send it via regular mail, the application can be downloaded from www.cms.hhs.gov/cmsforms. When you access the site, click on “CMS Forms.” Doing so will take you to a list of forms that includes the NPI application—CMS Form #10114. The application form is three pages long followed by instructions for completing the form. Individuals who render health care services are asked to complete Sections 2A, 3, 4A and 5.

Application Form Submitted by an Employer

In some cases, a psychologist who is employed by a health care entity may find that the entity is willing to submit the NPI application on his or her behalf. For example, a hospital may do so for its...
Final HIPAA Enforcement Rule Takes Effect

If you thought that the federal Health Insurance Portability and Accountability Act (HIPAA) lacked the “teeth” of enforcement, think again. The federal government has issued regulations that establish how the U.S. Department of Health and Human Services (HHS) will determine liability and calculate fines for health care professionals who violate any of the HIPAA Rules.

The HIPAA Enforcement Rule took effect in March 2006. The rule makes enforcement regulations applicable to all of the major HIPAA rules, including the Privacy and Security rules.

The HIPAA regulations pertain to covered entities including health care professionals whose activities “trigger” HIPAA. This happens, for example, when a psychologist transmits protected health information in submitting health care claims electronically. (See the article “What Triggers the Need to Comply?” on page 6 for additional information about actions that trigger HIPAA.)

This article highlights additional important aspects of the new Enforcement Rule that are important to psychologists: the general enforcement approach, liability for the acts of agents, fines and defenses available to a covered entity that is facing a penalty.

General Enforcement Approach

In deciding where to direct its enforcement efforts, HHS will rely primarily on complaints brought to the agency’s attention. However, HHS can conduct compliance reviews on its own if there has been no complaint. When acting on complaints, HHS is not limited to complaints by patients. For example, HHS can act on complaints from other covered entities.

Enforcement actions will remain private until a final penalty is imposed. So the fact that you may not have heard about HHS conducting investigations does not mean they are not taking place.

The Enforcement Rule generally favors a voluntary approach to HIPAA compliance whereby HHS would work with a psychologist at issue to make sure that the practitioner understands and corrects the violation. However, if such voluntary efforts fail, the rule calls for the agency to resort to investigations, hearings and fines.

Liability for Actions of Your Agent

The Enforcement Rule explains the circumstances under which you could be held liable for HIPAA violations of your agent—that is, someone acting on your behalf and at your direction. You can be subject to this type of “agency liability” if a member of your “workforce” commits HIPAA violations. The rule defines “workforce members” as including not only your paid employees, but also trainees and volunteers who are under your direct control.

You can also be held liable for violations by your agents who are not under your direct control but who are still carrying out HIPAA-related functions on your behalf. This kind of agent is generally considered a “business associate” under HIPAA. A person or company with whom you share protected health information as part of running your business, examples include a billing service or accountant.

There is an important exception to HIPAA liability provided by the Enforcement Rule. You generally are not liable for the HIPAA violations of your business associate if you are in compliance with the business associate provisions of the Privacy and Security Rules as they apply to your practice. Essentially, this means that you have in place “business associate contracts” that comply with those rules. Importantly, however, this exception will not protect psychologists who are aware that their business associates are violating the privacy or security obligations under their contracts and fail to take reasonable steps to remedy the problem.

One place to find a business associate contract that satisfies both the Privacy Rule and Security Rule is in the HIPAA Security Rule Online Compliance Workbook available online at APAnpractice.org.

Fines

The new Enforcement Rule allows HHS to impose fines of up to $100 per violation, to a maximum of $25,000 for violations of an identical requirement during one calendar year. A continuing violation is deemed a separate violation for each day it occurs. Thus, a continuing violation found to have lasted most of the year (at least 250 days) would reach the $25,000 limit for that one violation. In calculating the number of violations, HHS can rely on statistically valid sampling. However, the rule gives the accused entity a procedure for challenging those statistics.

HHS indicates that one act could give rise to several violations. The agency gives the example that the single act of disposing of a computer without first “scrubbing” the hard drive to remove electronic protected health information would violate several different HIPAA provisions.

In considering the amount of the fine, HHS will consider the nature and circumstances of the violation, the health professional’s history of prior compliance and his/her financial condition. More detailed considerations under the last category include the size of the covered entity and whether the fine would put the entity out of business.

When a proposed penalty becomes final, the enforcement process finally becomes public. HHS must notify the public of the fine imposed and the reason for imposing the penalty. HHS will also give notice to various other entities, including the appropriate state or local licensing agency and “the appropriate state or local medical or professional association.”

Available Defenses

The Rule provides several defenses that are available to someone facing a fine. If the fact that you may not have heard about HHS conducting investigations does not mean they are not taking place.

Enforcement actions will remain private until a final penalty is imposed. So the fact that you may not have heard about HHS conducting investigations does not mean they are not taking place.

Enforcement actions will remain private until a final penalty is imposed. So the fact that you may not have heard about HHS conducting investigations does not mean they are not taking place.

Enforcement actions will remain private until a final penalty is imposed. So the fact that you may not have heard about HHS conducting investigations does not mean they are not taking place.

Enforcement actions will remain private until a final penalty is imposed. So the fact that you may not have heard about HHS conducting investigations does not mean they are not taking place.
The APA Practice Organization is actively monitoring the potential for misuse of taxonomy code information and intends to take necessary actions to address any unintended uses of the taxonomy codes. But the fact of the matter is that, at the present time, we just do not know how payers may use this information.

With this as background, the APA Practice Organization evaluated the issue of choosing taxonomy codes and has identified at least three strategies.

Choosing Your Strategy

One strategy would be to choose all the taxonomy codes that represent any area in which you practice. For example, an insurer might deny payment for services that a psychologist provides to children when a practitioner chose the “child, youth and family” taxonomy code. This may protect you against being pigeonholed into a particular specialty area. However, there could be a risk of payment denials if an insurer decided to only pay for services in a particular practice area when the services were furnished by psychologists who identify themselves as specializing in that area--such as only paying for services to children when a practitioner chose the “child, youth and family” taxonomy code.

A second strategy would be to list only the general “psychologist” or “neuropsychologist” code. This may protect you against being pigeonholed into a particular specialty area, but the fact of the matter is that, at the present time, we just do not know how payers may use this information.

A third strategy would be to choose the code or codes that most accurately reflect your practice in its entirety, that is, the services you spend the majority of your time providing. For example, licensed psychologists with a broad-based practice might elect to choose just the “psychologist” code. On the other hand, psychologists who focus in specific practice areas may want to choose a specialty code or codes in addition to a general code. For example, a neuropsy-
A psychologist who focuses on providing services to geriatric clients may wish to choose the general “neuropsychologist” code as well as the specialty code, “adult development and aging.” If that neuropsychologist also furnishes services such as psychotherapy, feedback and/or cognitive rehabilitation, he or she may also want to choose the “clinical psychologist” code.

The APA Practice Organization generally advises practitioners to take the third approach. Though no strategy is risk-free, this option represents a balance of the first two strategies and may minimize the risk of negative reimbursement consequences until we have a better sense of how insurers will handle these codes.

Guidance from the APA Practice Organization may change when it becomes clearer how insurers will handle the codes. The NPI process permits practitioners to add or delete codes at any time.

The APA Practice Organization has expressed concern to the organizations involved that the taxonomy code list in its present form is inconsistent with the way that psychology is practiced. We are continuing to communicate with these groups in seeking appropriate revisions to the code list. We will apprise our members of future changes. We also stand ready to respond to any instances in which insurers use the taxonomy codes in inappropriate ways, so please notify the Practice Directorate if you encounter this situation.

Q. May I change my choice of taxonomy code?
A. Yes. Psychologists who have an NPI can change their taxonomy code designation at any time. The APA Practice Organization will update members if there are changes in taxonomy codes and/or our guidance for practitioners about selecting a code.

Do you have a question about the NPI that is not answered in this article? If so, contact legal and regulatory affairs staff for the APA Practice Organization by sending an email to practice@apa.org.

Online Resources for More Help with HIPAA

APApractice.org, the APA Practice Organization’s site, has a section with information and resources devoted to HIPAA compliance. In addition to the HIPAA Privacy and Security Rule, this section of APApractice.org includes information about a third rule that applies to practitioners: the HIPAA Transaction Rule. Click the button for the APApractice.org Store to access the following step-by-step compliance products developed specifically for practicing psychologists: HIPAA Online Privacy Rule Compliance Course (developed in collaboration with the APA Insurance Trust) and the HIPAA Security Rule Online Compliance Workbook.

The U.S. Department of Health and Human Services has a Web page located at http://www.hhs.gov/ocr/hipaa with answers to frequently asked questions about HIPAA privacy and other educational materials.

The U.S. Centers for Medicare and Medicaid Services devotes a portion of its Web site to HIPAA. Begin your search for general information at the following link: http://www.cms.hhs.gov/HIPAAGenInfo. For particular help determining whether you are a “covered entity,” type in the following address once you open your Web browser: http://www.cms.hhs.gov/apps/hipaa2decisionsupport/default.asp.

The following online resources are useful for practitioners in applying for a National Provider Identifier (NPI; see “Applying for Your National Provider Identifier,” page 14). Psychologists may complete and submit the NPI application form online at https://nppes.cms.hhs.gov. For those who wish to complete a hard-copy version of the application form and send it via regular mail, the application can be downloaded from www.cms.hhs.gov/cmsforms.