

HIPAA: Privacy Officers¹

Samuel Knapp, Ed.D.

Previous articles in the *Pennsylvania Psychologist* have given an overview of the origins and requirements of the HIPAA Privacy Rule (Knapp, 2002a; Knapp, 2002b). As noted in those articles, one of the responsibilities under HIPAA's Privacy Rule is to appoint a "privacy officer." This article briefly reviews the responsibilities of that privacy officer.

According to the HIPAA regulations, "a covered entity must designate a privacy officer who is responsible for the development and implementation of the policies and procedures of the entity" (45 CFR 164.530 (a) (1)). The duties of the privacy officer are to: (1) receive complaints and to provide further information about notice matters; (2) train members of the work force; and (3) ensure the compliance of the organization with privacy rules.

However, the implementation of privacy rules are "scalable," meaning that they vary according to the size of the organization. For a large organization with thousands of employees, the job of a privacy officer could entail a full-time position and perhaps some assistants. Psychologists in solo practice will be their own privacy officer. care previously given to patient information. The Privacy Rule will require substantial changes for large organizations, such as health insurers, who are not used to handling health care information with the same degree of care as mental health professionals are.

¹ Appreciation is expressed to the APA Practice Organization and the APA Insurance Trust (APAIT) for allowing us to adapt the materials that they have provided. The APA Practice Organization and APAIT will be making detailed forms (sample privacy notices, etc.) needed for HIPAA compliance available to its members or insureds for a nominal fee (non-members or non-insureds may purchase those materials at a higher cost). The target date for the availability of those materials is December 2002.

For psychologists who are used to treating patient information with great care the changes required by HIPAA should not be burdensome.

Receiving Complaints and Providing Further Information About Notice Matters

The privacy officer must receive complaints about perceived violations of patient privacy. Large organizations may need formalized procedures with specific forms and an advisory committee to review complaints. Psychologists in individual practices could best receive complaints by talking to the complainant directly and may only need to keep one “HIPAA Complaint File.”

Both large organizations and individual psychologists must attempt to mitigate any harmful effects when information is used without authorization. In a large organization there is a greater risk of leaks because the health care information may be shared with many individuals and the leak could involve many patients; whereas violations in the practices of individual psychologists would likely involve only one or a few patients.

Both the large organization and solo practitioner need to have predetermined sanctions against employees who fail to comply with the privacy policies. However, both would probably want to have progressive disciplinary measures that first emphasize education and only involve suspension or termination for repeated or egregious acts. Both large organizations and individuals are prohibited from intimidating, threatening, or discriminating against any individual who files a complaint, assists in an investigation of a complaint, or opposes any action made unlawful by HIPAA.

The privacy officer should also be available to provide further information to

patients about the privacy policies of the covered entity or to answer questions about the content of the privacy notice which is given to each patient at the start of treatment.

Training Members of the Workforce on Privacy

The covered entity must train all members of its workforce on the policies and procedures with respect to protected health information. All employees must receive the training before the compliance date (April 14, 2003). In addition, new employees must receive the training within a “reasonable period time” of starting their employment. That training must be documented.

For a large organization with thousands of employees, the training might involve a large auditorium and a lecture that may be supplemented with computer based programs, tutorials for supervisors, and extensive handbooks. For the individual psychologist, it may mean a sit-down conversation with the secretary. Materials that will be provided by APA and APAIT may assist psychologists in determining which topics to cover in that training. Since most psychologists have already trained their employees in confidentiality, the additional training required by HIPAA should not be burdensome.

Large organizations may need to supplement the training with reminders, update meetings, or posters. The individual psychologist may only need to comment to his or her employee once in a while if needed. For a large organization, the training might involve detailed instructions in the electronic security needed for the sophisticated computer system. The individual psychologist may have no such sophisticated computer system and, if records are kept on computer at all, would probably just be on a series of

diskettes kept under lock and key.

Both large organizations and individual psychologists should document the training and keep copies of the handouts or other educational materials.

Ensuring Compliance with the Privacy Rules

Regardless of the size of the organization, the covered entity is bound by the privacy practices as stated in its privacy notice. For example, confidential patient records need to be protected from access by unauthorized persons. The privacy officer in a large organization may need to walk through the company with a checklist to ensure that standards are being met. The individual psychologist can observe the privacy implementation as a matter of course in the day-to-day practice.

Large organizations may have to make extensive efforts to ensure that it is complying with the privacy standards. Independent psychologists who handle confidential information themselves will know whether or not they are following the privacy standards. Large organizations may have to enlist the input of workgroups before changing their privacy policies, and ensuring that they get implemented. Independent psychologists may only need to make the changes on their word processor and have them copied.

References

Knapp, S. (2002a May). An overview of HIPAA. *Pennsylvania Psychologist*, 62, 11, 21.

Knapp, S. (2002b October). HIPAA checklist. *Pennsylvania Psychologist*, 62, in press.

CE Questions

1. The duties of the privacy officer are to:
 - a. Receive complaints
 - b. Train members of the workforce
 - c. Ensure compliance with privacy rules
 - d. All of the above

2. The term “scalable” means that the duties of the privacy officer
 - a. Should involve scales of compliance
 - b. Vary according to the size of the organization
 - c. Are overlapping, like the plate-like structures on lizards
 - d. None of the above

3. Psychologists in solo practice should be advised to develop a standing advisory committee to assist them on complying with the Privacy Rules

TRUE

FALSE

4. It is recommended that the disciplinary actions against employees who violate privacy rules should
 - a. Be immediate and severe
 - b. Be scalable according to the size of the organization
 - c. Emphasize education first
 - d. None of the above

Answers:

1. D
2. B
3. False
4. C