What Should Your Employees Know About Confidentiality?

A HIPAA Training Guide

The HIPAA Privacy Rule requires employers to train all employees on the use of confidential information. “A covered entity must train all members of its workforce on the policies and procedures with respect to protected health information required by this subpart, as necessary and appropriate for the members of the workforce to carry out their function within the covered entity” (45 C. F. R. 164 530 (b) (1)). This does not mean that every employee must know everything about HIPAA and patient privacy; they only need to know what is necessary for them to carry out their duties. This training must occur for all employees before the compliance date or to each new employee within a reasonable time after they join the workforce.

This handout includes the minimum amount of information that most employees of psychologists need to have concerning confidentiality and patient privacy. Employers may use the information here as a guide when training their employees (or when they delegate the training of employees to others). However, some information, such as how to structure patient charts, can only be determined by the individual employer.

Employers/trainers can, if they like, use the questions at the end of this handout to test the degree to which their employees have mastered the material. Or employers/trainers may use a direct oral examination to test their mastery of this material. This training must be documented (employers/trainers may use the documentation form in this handout).

If employers/trainers choose to use the questions at the end of this document, then we would suggest that they establish a passing score ahead of time. We also suggest that employers/trainers allow the possibility that employees will get some questions wrong (even conscientious learners sometimes misread questions if they are nervous). If the employees fail the test, then the employers/trainers can allow them to retake the test. Employers/trainers can go over specific test questions with the employees afterward to ensure that they understand the material, or the employer/trainer can determine that the questions that they missed were unrelated to their actual job requirements.

The actual training involved may vary according to the needs of the covered entity or the responsibilities of the employee. For example, a records officer at a large hospital may need more extensive information than the secretary in the office of a solo practitioner. Professional employees should have a more detailed and thorough knowledge of privacy and confidentiality rules. Some employees may need less information than what is presented here.

This program will cover topics such as the philosophy behind confidentiality, the legal mandates behind confidentiality, the general nature of and rules regarding the Privacy Notice, how to handle requests for information such as through authorizations or court orders, how to store records and ensure privacy within your office, and what to do if a patient complains.
HIPAA Training Guide for Employees of Psychologists

Introductory Comment

The goal of this training guide is to give basic information about patient confidentiality and privacy. It is one of the requirements of the Health Insurance Portability and Accountability Act of 1996 that all employees of psychologists covered by the act have to be trained in privacy matters and that training has to be documented.

Because of the unique demands of your position, your employer may require that you learn additional information.

Most of the situations regarding patient privacy or confidentiality are predictable and foreseeable. However, you may encounter situations when the correct response is not obvious. *When in doubt, consult with your employer or the Privacy Officer.*

Philosophy Behind Confidentiality

Confidentiality is a general term for the promises of psychologists to keep information about patients private. Respecting confidentiality allows patients to be more willing to share information, even highly sensitive information, because they know it will be kept private. The quality of treatment would be seriously compromised if psychologists could not ensure confidentiality of these communications. It also shows respect for patient autonomy to give control of the information to the patient (there are a few narrow exceptions).

An effort to protect patient privacy reflects an intention to protect the dignity of our patients and to ensure that they receive quality treatment. Patient privacy is the responsibility of everyone in the office. In the ideal environment, all of the staff (clerical, billing, professional, custodial) will be looking out for the welfare of the patient and for each other. When there are threats to confidentiality, staff should feel comfortable in addressing it with each other. All of us are human and, under the right circumstances, may be unaware of how our behavior presents a risk to confidentiality.

The philosophy of protecting patient privacy should permeate the entire office from the time the patient first contacts the office. For example, staff should get permission before leaving messages for patients at their homes or on their answering machines.

Staff should not gossip about patients. They should not disclose any identifiable patient information outside of the office. It is a small world and information that you may consider innocuous may be identifiable or give an impression to the public that confidentiality is not important. In social settings you should only give out general information about your work. When in doubt, be silent.
Legal Mandate Behind Confidentiality

Confidentiality rules were originally found in the code of ethics of psychology, but they have been embodied in law through the regulations of the State Board of Psychology, malpractice courts, and now through HIPAA’s Privacy Rule. Psychologists who breach confidentiality could be disciplined by a state board of psychology, an ethics committee, or be liable for damages in a malpractice suit, or investigated by the Office of Civil Rights of the Department of Health and Human Services, which is the federal agency responsible for enforcing HIPAA.

Psychologists are obligated to ensure confidentiality of communications and may also be sued themselves for breaches of confidentiality by their employees. HIPAA requires that all employees undergo training in confidentiality and privacy procedures. Employees who violate patient confidentiality could be subject to disciplinary actions. Employees who are uncertain about how to respond in a particular situation should consult with their employer or Privacy Officer.

What is HIPAA?

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) contained numerous insurance provisions, but the one relevant here is the Privacy Rule, which mandates that “covered entities” (such as health care providers who disseminate information electronically) have to meet certain minimal standards of patient privacy including giving a privacy notice to all patients, having certain minimum standards on all patient authorizations (release of information forms), having agreements with business associates to ensure the protection of patient privacy, and appointing a privacy officer for every covered practice.

Fortunately, HIPAA’s implementation is “scalable,” meaning that the requirements for compliance can vary according to the size of the organization. For example, whereas a large hospital may have to have a full-time Privacy Officer, psychologists in solo practices will be their own privacy officers. Also, HIPAA follows a preemption analysis whereby state laws preempt HIPAA if they are more protective of patient privacy from the standpoint of the patient. Almost all state laws dealing with mental health are more protective of patient privacy and will therefore stay the same.

The Privacy Notice

HIPAA requires every health care provider to present clients/patients with a privacy statement that reviews, in language understandable to the average person, the relevant limitations on privacy. Some psychologists may want to give the Privacy Notice at the same time they give an informed consent or service brochure to patients, although the two forms may not be combined. The Privacy Notice may, but does not have to be, layered (have a brief summary on
HIPAA’s Privacy Rule requires that all patients must be given a Privacy Notice at their first encounter except for emergencies. Phone contacts to schedule appointments are not considered the first encounter.

What should you do if a patient refuses to sign? There is no penalty to providers who demonstrate good faith efforts to get the signature. Psychologists should document “good faith” efforts to get the signature.

The Privacy Notice includes information on use of disclosures and authorizations (corresponds to what psychologists call “release of information forms”), the patient’s rights to records, and rules regarding access to records. Depending on state law, these rules of access do not include psychotherapy notes (they do apply to test results and other health care information), the right to request to amend the records, and accounting of sharing Protected Health Information (PHI). The accounting does not have to include disclosures made on the basis of a patient authorization.

The Privacy Notice has to be posted where patients can see it.

Patients need to receive only one Privacy Notice for every legal entity from which they receive treatment. For example, a patient needs to receive only one Privacy Notice if she receives both the psychotherapy and medications from the same agency.

If you are uncertain how to respond in any situation dealing with the Privacy Notice, you should consult with your employer or Privacy Officer.

Requests for Information

This section provides general information about subpoenas, court orders, and patient authorizations. Your employer will determine your responsibilities for responding to these requests for information. When you have any questions or uncertainties about how to handle a particular situation you should consult with your employer or Privacy Officer.

Subpoenas and court orders

A subpoena is a request for documents served by an attorney. Often attorneys will utilize a record copying service to secure these records. Psychologists may not release information in response to a subpoena alone. Instead, psychologists may release information only in response to a valid authorization (release of information form) from the patient or a court order. Although psychologists need to respond to every subpoena, their response may be as simple as “I cannot release information without a signed release from the patient or a court order.”
Many psychologists prefer that they, and not administrative staff, make all decisions concerning responses to subpoenas and court orders. 

**Authorizations (Release of Information forms).**

Authorizations are generally required to release information to outside agencies. Psychologists, however, may share information with students, trainees, and supervisees without getting a patient authorization. Authorizations for psychotherapy notes may not be combined with authorizations for other health care information. That is, the request for psychotherapy notes cannot be made on the same authorization form as a request for other health care information.

Other decisions about a few narrow exceptions to confidentiality have to be made by the psychologist. These may include the mandated reporting of child abuse, the duty to warn or protect when there is imminent danger to the safety of an identifiable third person, or whether or not to report elder abuse.

**Keeping Privacy Within the Office**

**Record Retention and Access**

You need to keep records in a secure location out of contact from patients or other members of the public. Charts or other confidential information should not be left around where patients or other personnel could see them. File cabinets should be locked when not in use.

Your employer will give you more detailed information concerning how to keep charts including information on where specific pieces of information can go on those charts.

**Business Associates**

Business associates are individuals who do not provide health care services, but who have a legitimate need for a limited amount of Protected Health Information. The term “business associates” could include attorneys hired by your employer, billing services, or others. Your employers should have a business associate contract which allows them to send limited information and which obliges them to respect the privacy of patient information. The information sent to business associates should be the minimum necessary for them to fulfill their responsibilities.

**Controlling Accidental Breaches of Information**

Staff needs to pay attention to inadvertent breaches of privacy in the waiting room (such as through conversations leaking through offices, or visibility of appointment books in the waiting room or information on a computer screen).
You should be alert to any situations where information can be accidentally leaked and you should be open to suggestions from others about how you might have done something that could have accidentally leaked information. Patient privacy is everyone’s concern.

**What to Do If a Patient Complains**

Every covered entity must have a process for individuals to make complaints concerning how confidential information was handled. These complaints would typically be handled by a “Privacy Officer” who is an employee of the organization (usually a psychologist, but not necessarily) who provides a process by which the grievance can be heard and addressed.
Other Topics

Consent for Recording Information

Psychologists need to get special consent for recording the voice or image of a patient.

Policies on Electronic Transmission of Information

Institutions vary on their policies concerning acceptance or transmission of information electronically, such as through e-mail. You should know your employer’s policy. If your employer does allow for the transmission of electronic information, patients need to be notified of any limitations to confidentiality on transmissions they send or receive from your office.

Other Topics Unique to Your Practice

There may be other topics unique to your practice that you need to discuss with your employees.
Confidentiality Training Verification

On ____________________, I reviewed the following rules regarding confidentiality with

(Date)

my employee__________________ and she or he understood the general principles that

(Name)

were taught.

___The Philosophy Behind Confidentiality
___The Legal Mandates Behind Confidentiality
___What is HIPAA?
___The Privacy Notice
___Requests for Information
___Keeping Privacy Within the office
___What to Do If a Patient Complains
___Other Topics Unique to Your Practice

(Please specify)__________________________________________________________

__________________________________________________________

________________________________
signature of psychologist or Privacy Officer
Employee Test on Confidentiality and Privacy Issues

1. Confidentiality refers to the
   a. Absolute right (with no exceptions) to freedom from unnecessary intrusion in our lives
   b. Right of patients, under all circumstances, to keep information out of court
   c. Promise on the part of psychologists to keep information private
   d. All of the above

2. A psychologist who violated the rules regarding patient confidentiality could be
   a. Disciplined by an ethics committee
   b. Disciplined by the state board of psychology
   c. Sued in a malpractice court
   d. All of the above

3. The responsibility for ensuring confidentiality in an office rests with
   a. The patients
   b. The Privacy Officer alone
   c. All staff
   d. Only psychologists or social workers.

4. The rules for confidentiality can be found in
   a. The APA Code of Ethics
   b. The regulations of the State Board of Psychology
   c. HIPAA’s Privacy Rule
   d. All of the above

5. The Privacy Notice must be given to patients
   a. At the time they start treatment (except in emergencies)
   b. Along with an informed consent document
   c. As soon as they call on the phone and ask for their first appointment
   d. At the end of treatment

6. A layered Privacy Notice is one that
   a. Can be peeled away like several layers of an onion
   b. Includes a brief summary at the beginning and the more detailed description later
   c. Contains far more information about privacy than anyone would want to know
   d. None of the above
7. Psychologists must turn over records in response to a
   a. Subpoena
   b. Court order
   c. Verbal request from a physician
   d. None of the above

8. What statement best describes the information that may be sent to business associates?
   a. They have access to all information
   b. They should have access to information only with a specific authorization from the patient
   c. They may not have access to information
   d. They may have access to the minimum amount of information about patients necessary for them to fulfill their responsibilities.

9. What are some ways that patient information may accidentally get leaked in an office?
   a. Charts are left lying on unattended desks
   b. Patients accidentally look into the appointment book
   c. Conversations in private offices “leak” into the waiting room.
   d. All of the above

10. The Health Insurance Portability and Accountability Act (HIPAA) requires that
    a. All “covered entities” have exactly the same procedures for charting patient records
    b. Business associates have access to all patient information
    c. Records have to be kept a minimum of seven years
    d. None of the above

True or False

11. Staff should not reveal identifying information about patients outside of the office except for professional purposes and a patient authorization or legal justification.
    TRUE      FALSE

12. The general rule is that psychologists are liable for the actions of their employees.
    TRUE      FALSE

13. A Privacy Notice may be given at the same time as an informed consent form, although the forms must be separate.
    TRUE      FALSE
14. A hospital must provide a patient with a new Privacy Notice for every health provider that delivers services to them.

TRUE     FALSE

15. Psychologists must get authorizations signed by patients in order to share information with their supervisees.

TRUE     FALSE

Test Answers

1. C
2. D
3. C
4. D
5. A
6. B
7. B
8. D
9. D
10. D
11. TRUE
12. TRUE
13. TRUE
14. FALSE
15. FALSE