

## **HIPAA and Pharmacy Practice for the Pharmacy Technician**

**Edward D. Rickert, B.S. Pharm., J.D.**

You may have noticed some changes in the way that prescription information has been handled in your pharmacy since April 14, 2003. The reason for the changes is that on that date, the privacy standards under the federal Health Insurance Portability and Accountability Act (“HIPAA”) took effect. If you were aware of HIPAA prior to April 14, 2003, you likely feared the coming changes, and the effect those changes would have on how pharmacy was practiced in your work setting. You likely dreaded the increased work load, patient (and practitioner) confusion over the rules, and general state of chaos that many predicted would follow the implementation of the privacy standards. However, if you have lived and worked under those standards for the past several months, you will likely agree that, to paraphrase that Mark Twain, rumors of the death of pharmacy as a result of the new federal mandate have been greatly exaggerated.

Although the new federal law has imposed new record keeping, notice and accountability requirements on the profession, the main purpose of the federal privacy regulations, which is to require pharmacies to treat patient information confidentially, is nothing new. Most state laws and the codes of ethics governing the profession both address the need for confidentiality in the pharmacy. In Illinois, “confidential information” acquired by the pharmacy for use in connection with providing pharmaceutical care is defined as “information, maintained by the pharmacist in the patient’s records, released only (i) to the patient or, as the patient directs, to other practitioners and other pharmacists or (ii) to any other person authorized by law to receive the information.” Illinois Compiled Statutes, 225 ILCS § 85/3(p). Your training as a technician, even before April 14, 2003, should have included instruction on the importance of maintaining the confidentiality of health care information. The general rule is now, and has always been, that you are to keep confidential health care information confidential. You cannot use or disclose a patient’s health care information for purposes other than providing health care to the patient, obtaining payment for the health care services provided, and in connection with the day to day operations of the pharmacy.

The basic premise that health care information should be maintained in confidence was stated in the Illinois pharmacy laws in just forty simple words. In implementing the HIPAA privacy standards, the federal government formalized this basic concept in the form of regulations that are 401,034 words in length! To put that in perspective, this article is roughly 5,000 words in length. The purpose of this article is to summarize the federal government’s 401,034 words in simple terms, and to explain how those words impact your practice as a pharmacy technician.

### **What is HIPAA?**

HIPAA stands for the Health Insurance Portability and Accountability Act, and is a federal law that was passed by Congress in 1996. The original intent of the legislation was to address the problem of “job lock”. Job lock occurred when a person was unable to

leave his or her job for a new job when, due to a health condition of the employee or a member of the employee's family, changing jobs would result in an inability to obtain health insurance through the new employer. HIPAA was also a part of the Clinton Administration's efforts to enact legislation providing for universal health care coverage for all Americans.

In what may be one of the great misnomers of all time, the privacy portion of the new law is found under the section entitled "Administrative Simplification". The purpose of the Administrative Simplification provision was to make it easier and less expensive for health care providers and health care plans to transmit and receive health information electronically. The rules (all 401,034 words of them) that implement the "Administrative Simplification" provisions are complex and often confusing. However, if you rely on common sense, and are mindful of the primary purpose of the regulations, which again is to maintain the confidentiality, and to limit the use and disclosure of a patient's health care information, the regulations become more understandable and manageable.

In addition to the privacy mandate, the Administrative Simplification provision requires health care providers to comply with certain security requirements, and when transmitting data electronically, to comply with certain format requirements. Those requirements are set forth in separate regulations, and are not addressed in this article.

### **Who is Covered By HIPAA?**

The HIPAA privacy rules apply to "covered entities". "Covered entities" are health care providers, health plans, and health care clearinghouses. In your position as a pharmacy technician, you should know that a pharmacy is a "health care provider", and that as an employee of the pharmacy, you are covered under HIPAA. You should also recognize that a "health plan" includes third party payers that provide health care coverage, including plans that pay for a patient's prescription medications.

The reason this is important is two-fold. First, as an employee of a "health care provider", you are required to comply with the HIPAA privacy standards. Next, since health plans are also "covered entities" that are required to comply with HIPAA, you should take comfort in knowing that health information that you provide to the health plan should be treated by the plan confidentially, and in compliance with HIPAA.

A "health care clearinghouse" is an entity you may not be familiar with. A health care clearinghouse is an entity that facilitates the processing of health information from non-standard format or content to a standardized form, and vice versa. This includes a billing service used by a pharmacy, that converts billing information maintained in the pharmacy to a standardized electronic form that can be used by the payer.

A pharmacy that is located in a hospital is a covered entity under HIPAA. However, a hospital and its various departments and affiliated groups are treated under the HIPAA rules as an "organized health care arrangement", and the responsibility for complying with the privacy rules is shared by the parties to that arrangement. Many of the

administrative tasks associated with ensuring HIPAA compliance in the hospital setting are performed by the hospital, and not by the pharmacy or pharmacy staff. Although for ease of reference, this article refers to “pharmacies” as having certain responsibilities under HIPAA, the reader should be mindful of the fact that in the hospital setting, the pharmacy falls under the hospital’s HIPAA umbrella, and many of the responsibilities will fall on the shoulders of the non-pharmacy hospital staff.

### **What Type of Information is Covered By HIPAA?**

The HIPAA privacy rules provide protection against the use and disclosure of “protected health information” (“PHI”). Health information is protected if it is (1) created or received by a covered entity; (2) relates to an individual’s past, present or future physical or mental health condition; and (3) identifies the individual or creates a reasonable basis to believe that the information can be used to identify the individual. Health information that meets this criteria is deemed to be “individually identifiable”, and is protected under HIPAA. Information that merely includes information about an individual’s health condition, without any information that could be used to identify the individual, is not PHI.

Thus, for example, a record containing the name of a person along with that person’s medical diagnosis – Mrs. Jones has high blood pressure – is clearly individually identifiable health information protected by HIPAA. A prescription for Mrs. Jones for propranolol would also be individually identifiable health information. A reimbursement request sent to a third party payer, which identifies Mrs. Jones and the medication dispensed is also individually identifiable, and therefore protected. These are obvious examples.

However, what about a record that identifies only an unnamed female born on July 4, 1935, who has been prescribed propranolol? Or a record that discloses that a person residing in the 60516 zip code is being treated with propranolol? Surprisingly, such records may be considered to be individually identifiable health information. The regulations provide a list of eighteen “identifiers” that must be removed in order for a covered entity to determine that health information is not identifiable to an individual. The list includes obvious identifiers, such as the person’s name, social security number, telephone number, and email address, which can clearly be used to identify an individual. However, the list also includes less obvious “identifiers”, including the individual’s city, county, precinct, or zip code. Information that includes health information, along with any of the eighteen identifiers may be considered to be individually identifiable, and therefore protected under HIPAA.

Next, it is important to note that individually identifiable health information transmitted in any form – on paper, electronically or even orally – is protected. Thus, in addition to obvious records such as prescriptions, patient profiles, and billing forms, verbal communications, such as telephone calls received in the pharmacy, and patient counseling, can also be protected health information. Reasonable care must be taken to limit the use and disclosure of PHI in connection with these two types of transactions.

## **What Does HIPAA Require?**

The HIPAA privacy rules impose upon covered entities specific requirements, which are designed to ensure that an entity does not use or disclose a person's PHI except as permitted or required by the rules. In general, the requirements imposed on pharmacies and pharmacists under HIPAA are:

- (1) To notify patients about their privacy rights, and about how their information can be used by the pharmacy;
- (2) To ensure that pharmacy personnel comply with HIPAA, by adopting and implementing privacy procedures for its pharmacy practice, and training employees so that they understand the those procedures;
- (3) To designate an individual to be responsible for seeing that the privacy procedures are followed; and
- (4) To secure patient records that contain individually identifiable health information so that they are not readily available to those who do not have a need to have access to them.

The notice requirement is perhaps the most important requirement, in that unless a pharmacy provides the proper form of notice to its patients, the pharmacy would be prohibited from using or disclosing PHI and, therefore, would be unable to practice pharmacy. The rules require notice to be provided by a document called the "Notice of Privacy Practices" ("NPP"). The pharmacy must provide the NPP to all patients, at or as near as possible to the time that the pharmacy service is first provided to the patient. The rules include specific requirements concerning the content of the NPP.

First, the NPP must contain the following mandatory statement, displayed in a prominent manner on the face of the document:

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU  
MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO  
THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

Next, the NPP must be written in plain language, and must convey the following information to the patient:

- (1) a description and at least one example of how the pharmacy will use the patient's PHI;
- (2) a statement of the types of uses and disclosures that require prior authorization from the patient;
- (3) a statement advising the patient that the pharmacy is required to maintain the confidentiality of PHI;
- (4) a statement of the patient's rights under HIPAA, including the right to request restrictions on the disclosure of PHI, the right to receive, inspect and copy PHI, the right to request amendments to PHI maintained by the

- pharmacy, and a right to obtain an accounting of certain disclosures of PHI made by the pharmacy;
- (5) a statement that patients may complain to the federal Department of Health and Human Services (“HHS”) if the patient believes that his or her HIPAA rights have been violated; and
  - (6) the identity of the pharmacy’s “privacy officer”, who is, under HIPAA, the individual responsible for ensuring HIPAA compliance for the pharmacy.

Generally, the NPP need only be provided to the patient one time, at or near the time that pharmacy services are first provided to the patient. However, if there is a material change in the content of the NPP, or in the way that the pharmacy intends to use and disclose PHI, a new NPP should be provided to the patient.

In addition to providing the NPP, the pharmacy is required to make a “good faith” effort to obtain a patient’s written acknowledgment of receipt of the NPP. The written acknowledgment can take the form of a signature log, kept at the pharmacy counter, but if such a log is used, it cannot be combined with a log used for other purposes, such as documenting a patient’s refusal to accept an offer of counseling. Once obtained, the authorization is to be maintained in the pharmacy for a period of six (6) years. If a patient refuses to sign an acknowledgment, or if the pharmacy is unable to obtain a signed authorization despite its good faith effort, then the pharmacy must make a record of that fact, and maintain that record for a period of six (6) years.

If a pharmacy has more than one location, such as a chain pharmacy, the NPP need be provided, and the written acknowledgment obtained, only one time, and at only one location. Similarly, if a pharmacy is part of an organized health care arrangement, such as a hospital pharmacy, the NPP need be provided, and the written acknowledgment obtained only once. For example, in a hospital setting, the admissions clerk will likely provide the NPP, and obtain the acknowledgment, at the time of admission, for all of the various departments that are part of the hospital.

### **How Can A Pharmacy Use and Disclose PHI Either With or Without Authorization?**

After providing the NPP, and making a good faith attempt to obtain a written acknowledgment, the pharmacy can use and disclose PHI without obtaining any consent or patient authorization, as long as the use and disclosure is for purposes of “treatment”, “payment”, or “health care operations” (referred to collectively as “TPO”). The overwhelming majority of uses and disclosures of PHI that occur in a pharmacy will fall within these three categories of activities. “Treatment” includes all activities associated with filling prescriptions or medication orders, including discussions concerning the drug therapy with prescribers and other health care professionals (such as nurses, laboratory technicians, etc.), drug utilization review activities, and dispensing the medication to the patient. “Payment” includes all communications required to obtain payment or reimbursement for the dispensing activities, including obtaining prior authorization from third party payers, claims submissions, and providing information to payers concerning

the patient's diagnosis and the use of the drug or the need for drug therapy. "Health care operations" are activities required for the day to day operations of the pharmacy, including record keeping, preparation and review of quality assurance reports, and risk management activities.

The use or disclosure of PHI for any purpose other than TPO will require the pharmacy to obtain written authorization from the patient *before* the PHI is used or disclosed. An example would include using PHI for marketing purposes. If a patient refuses to sign an authorization, the pharmacy is prohibited from using or disclosing the information, and the pharmacy may not condition treatment on the receipt of an authorization. It is important to note that certain activities that may appear to be "marketing" are in fact considered to be treatment, and do not require authorization. In a guidance document, HHS has stated that using PHI to provide refill reminders to a pharmacy patient, or to let the patient know about disease state management programs offered by the pharmacy, are considered to be treatment, and therefore do not require authorization.

The form of the authorization is addressed in the rules in general terms. The form must be a separately signed and dated document, and cannot be included as part of, or combined with any other form or document. It must stand alone, in order to minimize the likelihood of any confusion over the purpose of the authorization, or of the intended use of the PHI. The precise form the authorization must take is not specifically stated in the rules. However, the following information must be included: (1) a specific and meaningful description of the PHI to be used or disclosed; (2) the name(s) or specific identification of the person(s) or entities to whom the PHI will be disclosed; (3) a description of each purpose for which PHI will be used or disclosed; (4) an expiration date or event after which the authorization will no longer be valid; and (5) the patient's signature and the date signed. The authorization must be kept on file at the pharmacy for six (6) years.

Although the rules state that for all uses or disclosures other than TPO, an authorization must be obtained, it should come as no surprise that within the 400,000 plus words that comprise the privacy regulations, there are exceptions to this general rule. The HIPAA rules identify a number of non-TPO uses or disclosures that can be made without first obtaining the patient's authorization. These include:

- uses and disclosures required by law;
- uses and disclosures for public health activities;
- disclosures about victims of abuse, neglect or domestic violence;
- uses and disclosures for health oversight activities;
- disclosures for judicial and administrative proceedings;
- disclosures for law enforcement purposes;
- uses and disclosures about decedents;
- uses and disclosures for cadaveric organ, eye or tissue donation purposes;
- uses and disclosures for research purposes;
- uses and disclosures to avert a serious threat to health or safety;
- uses and disclosures for specialized government functions; and

- disclosures for workers compensation.

The rules do not clearly define the types of pharmacy related activities that would fall within these categories, and it will be years before this area is fully interpreted and defined. However, one example of an activity that would likely fall within the category of a “health oversight” activity would be allowing a pharmacy board inspector review prescription records. When an inspector visits the pharmacy, he has access to prescription records in order to monitor and assess the pharmacy’s compliance with the pharmacy practice laws and regulations. As long as the inspector is acting in the usual course of his or her regular activities on behalf of the pharmacy board, and is accessing no more information than is necessary to perform the task at hand, nothing in HIPAA would affect the inspector’s ability to perform his or her job.

The exception for health oversight activities is different from the exception for disclosures for judicial or administrative purposes. In most cases, in order to obtain PHI for use in connection with a court or an administrative proceeding, the party seeking the information would still be required to comply with the rules governing that type of proceeding, and would likely require a subpoena before releasing PHI.

### **Limitations on the Use and Disclosure of PHI**

The privacy rules impose certain limitations on the use and disclosure of PHI when a written authorization is not required. The rules provide that a pharmacy must make reasonable efforts to limit the use or disclosure of PHI to the minimum amount required to accomplish the purpose of the use or disclosure. This so-called “minimum necessary” standard does not apply to disclosures for treatment purposes, disclosures to the patient themselves, or to disclosures made pursuant to a written authorization from the patient.

Note that the minimum necessary standard does apply to disclosures for payment and health operations. Thus, when submitting a claim for reimbursement, the pharmacy can disclose only the minimum amount of information required to obtain payment. HHS has provided some written guidance on this issue, however, and suggests that as long as the pharmacy complies with HIPAA standards for electronic transactions, any PHI disclosed electronically for purposes of obtaining reimbursement would, by definition, be the minimum necessary.

Similarly, it would appear that the disclosure of PHI without authorization for health oversight, law enforcement activities, judicial or administrative proceedings, and any of the other activities identified in the preceding section, would be subject to the “minimum necessary” standards. Thus, for example, if a board inspector is investigating a dispensing error, but requests access to all records related to the dispensing of controlled substances, one could argue that the minimum amount of information necessary for the purposes of the investigation would be information related to the specific error under investigation. Again, this area of the HIPAA rules will likely be interpreted and developed through enforcement actions, further HHS guidance documents, and court proceedings.

Finally, since the minimum necessary standards do not apply to treatment activities, pharmacies can share information with a patient's doctors, nurses, or other health care providers, including other pharmacies, so long as the purpose of the release is related to the treatment of the patient. For example, at one point, it was believed by some that after April 14, 2003, if a pharmacy were to call another pharmacy to see whether a patient had been obtaining narcotic medications from the other pharmacy, the pharmacy would be prohibited under HIPAA from providing the information. A better view, however, is that dispensing narcotic medications requires good faith on the part of the pharmacist and technician, and the question of whether the patient has been obtaining similar medications from multiple pharmacies would be important information to know in connection with providing proper treatment for that patient. Accordingly, HIPAA would not prohibit the disclosure of that information, and the minimum necessary standards would not apply to such disclosures.

Another limitation that must be considered in connection with the use and disclosure of PHI is the need to take reasonable steps to ensure that access to PHI is limited only to those persons who have a right to access PHI. For example, a pharmacy may need lock prescription files, including older files that are no longer used in the pharmacy, to ensure that non-pharmacy personnel cannot access those records when the pharmacy is closed. When disposing of records containing PHI, care must be taken to "de-identify" the records, so that the individually identifiable information cannot be obtained. This can be accomplished by blacking out names and other identifiers on prescription vials before disposing them, or shredding paper PHI that is no longer needed.

It may also be necessary to issue computer passwords to pharmacy employees, to ensure that non-pharmacy employees cannot access the computer records of pharmacy customers. Care must also be taken to prevent incidental disclosures of PHI such as, for example, taking steps to prevent other patients from overhearing when the pharmacist counsels a patient at the pharmacy counter, or discusses a patient's medication therapy or health condition with a doctor or nurse, either over the telephone or in the pharmacy. The key here, however, is reasonableness under the circumstances. The rules and HHS guidance provides that secondary uses or disclosures that cannot be reasonably prevented, are limited in nature, and are a by-product of a permitted disclosure would not necessarily be found to violate the privacy rules. Thus, it is not necessary to construct a sound-proof room for patient consultations, but if counseling is performed in an area where the conversation could be overheard, efforts should be made to keep persons other than the person being counseled away from the area, and to speak in a quieter voice, so as to minimize the risk of an inadvertent, incidental disclosure.

### **What Are A Patient's Rights Under HIPAA?**

In addition to protecting PHI, the HIPAA privacy rules has other important features. A patient's rights concerning his or her PHI is just as important as patient privacy. As previously discussed, HIPAA requires that pharmacy patients receive notice of the ways that their health information will be used and disclosed by the pharmacy. Patients have

other rights under HIPAA. The HIPAA privacy rules provide patients with more control over their health information. Patient confidence in the integrity of the health care system is essential in order to encourage patient's to allow their health information to be released, without fear that the information will be misused.

In a pharmacy, it is common for patients to request a copy of their prescription record, or for a copy of an individual prescription. It is less common for a patient to request to review other information the pharmacy may be maintaining as part of its patient record. For example, under the pharmacy laws of every state, pharmacies are required to maintain a patient profile, which often includes information concerning a patient's allergies, medical diagnoses, and other information relevant to a patient's health. Under HIPAA, pharmacies are required to notify patients not only that such records are maintained in the pharmacy, but that, with a few exceptions, patients have a right to review that information, obtain copies, and to request amendments to those records if the patient believes that amendments are necessary.

When a patient requests access to or a copy of his or her pharmacy records, the pharmacy is required to respond to that request within thirty (30) days. A pharmacy can deny access to records in certain limited circumstances. For example, if the information sought was compiled not for health care purposes, but in anticipation of or for use in a civil, criminal, or administrative action or proceeding, the pharmacy may refuse to allow access to the information. Other exceptions exist, but they are very limited, and it is beyond the scope of this article to fully address those issues. Suffice it to say that each request for access to records should be reviewed on an individual, case by case basis, and that that in the overwhelming majority of cases, the request will be honored.

Patients also have the right to request that amendments be made to their records. The pharmacy can require that any requests that records be amended be made in writing. Once a request is made, the pharmacy must respond to the request within sixty (60) days. A pharmacy can deny a request for an amendment under the following circumstances:

- It is determined that the requested protected health information or record was not created by the pharmacy, unless the individual provides a reasonable basis to believe that the originator of the PHI is no longer available to act on the requested amendment.
- The record sought to be amended is not part of the pharmacy's "designated record set". A "designated record set" is a treatment or billing record maintained by the pharmacy and used in whole or in part to make decisions concerning the individual, such as, for example, prescription records, patient profiles or billing records.
- The record would not be available for inspection under the requirements for individual rights to access protected health information, such as, for example, a record created in anticipation of litigation.
- It is determined by the pharmacy that the record is accurate and complete.

To illustrate how a request for an amendment might work, consider this example. A patient may believe, based on a review of his or her records, that information contained in the record is incorrect. For example, the record might identify a medication that the patient denies was ever obtained from the pharmacy, and ask that the record be amended to delete reference to that medication. The pharmacy may require that the request be made in writing. Upon receipt of the request, the pharmacy would be required to review the request, and the patient's records, and make a decision as to whether or not to comply with the request. If a review of the pharmacy's records reveals that an error had been made, the pharmacy would comply with the request and amend the record. For example, if there are two Mary Smith's who receive prescriptions at the pharmacy, and the profile for the Mary Smith who is requesting the amendment includes a prescription for Prozac that should have been entered on the other Mary Smith's profile, it would be reasonable for her to request an amendment to delete reference to that drug from her profile. The pharmacy should comply with the request, and amend the record. If, however, it appears to the pharmacy that no error was made, the pharmacy can deny the request.

Finally, a patient can request an accounting of disclosures of his or her PHI. Under the rules, the pharmacy is required to maintain a record of all disclosures other than those made to carry out TPO, disclosures to the individuals themselves, disclosures for national security or intelligence purposes, or disclosures to correctional facilities, as provided in the rules. A record of all other disclosures must be maintained for six (6) years.

For example, in the example used above, in which a prescription for Prozac was entered into the profile of the wrong Mary Smith ("Mary Smith No. 1") when that fact was brought to the attention of the pharmacy, a record should be created indicating that Mary Smith No. 1's use of Prozac was disclosed to another patient named Mary Smith. This accounting of this wrongful disclosure should be maintained by the pharmacy, and provided to Mary Smith No. 1 upon request for an accounting of disclosures.

### **What Are the Penalties for Violations of HIPAA?**

The federal government, as is evidenced by the penalties provided for non-compliance takes compliance with the HIPAA privacy standards very seriously. Under HIPAA, the federal government is permitted to impose civil penalties, as well as criminal penalties, for non-compliance.

Non-compliance can result in civil penalties of up to \$100 per violation and up to \$25,000 per person in any calendar year for the improper disclosure of PHI. If the disclosure was done intentionally, or with knowledge that the information was protected, but was nevertheless disclosed, criminal sanctions can be imposed. Penalties for an individual that knowingly permits uses or discloses PHI improperly can be as harsh as a \$50,000 fine, and up to one year in jail.

If an individual uses PHI under false pretenses, the penalty can increase to \$100,000 and/or up to five years in jail. Finally, fines of up to \$250,000 and/or ten (10) years in

prison can be imposed where the covered entity uses PHI for “commercial advantage, personal gain or malicious harm.”

During the first year of HIPAA, federal enforcement authorities have indicated that enforcement will be complaint driven, and will take a “fair and reasonable” approach designed to ensure future compliance. After the first year, all bets are off, and HHS may begin an aggressive enforcement campaign, and avail itself to the full range of civil monetary and criminal penalties. It would be wise to not risk enforcement, and becoming HIPAA compliant.

## **Conclusion**

Seven years after its passage, HIPAA is a reality, and has impacted the way that pharmacy is practiced. However, the HIPAA privacy rules have not proven to be as burdensome as some had feared. The use of common sense, and a concern for the confidentiality rights of pharmacy patients, will help guide you in ensuring that your practice is HIPAA compliant.

## **SELF-ASSESSMENT TEST**

Select the best answer to the following ten questions.

1. Which of the following would be considered to be a “covered entity” under the HIPAA privacy rules?
  - A. A pharmacy.
  - B. An insurance company that pays for a patient’s prescription medications.
  - C. A data processing company that receives data from a pharmacy, and transmits it in another form to the third party payer.
  - D. All of the above.
  
2. Which of the following information would be considered “protected health information”.
  - A. A prescription order faxed to the pharmacy by a doctor.
  - B. A record containing the number of propranolol prescriptions written by a specific doctor in a thirty day period.
  - C. A used prescription vial that has had the patient’s name blackened out from the label.
  - D. A list of all doctors within a hospital who treat migraine headaches.
  
3. Which of the following must be included in a “Notice of Privacy Practices” provided to a patient by a pharmacy?
  - A. A description of how the pharmacy will use the patient’s protected health information.

- B. A statement of the types of uses and disclosures that require prior authorization from the patient.
- C. A statement of the patient's rights under HIPAA.
- D. All of the above.
4. When is a pharmacy required to provide a Notice of Privacy Practices to a patient.
- A. Each time the patient visits the pharmacy.
- B. At or near the time that pharmacy services are first provided to the patient.
- C. In a hospital setting, each time the pharmacy sends a medication to the patient's room.
- D. Only if the patient requests a copy of the Notice.
5. How long is a pharmacy required to maintain a record of a patient's acknowledgment of receipt of the Notice of Privacy Practices.
- A. Two years.
- B. Five years.
- C. Six years.
- D. Ten years.
6. Under which of the following circumstances can a pharmacy release protected health information without first receiving prior authorization from the patient.
- A. When the information will be used for payment, treatment or health care operations.
- B. When the use or disclosure is required for health oversight activities.
- C. When the disclosure is required in connection with a judicial or administrative proceeding, typically pursuant to a subpoena.
- D. All of the above.
7. When must a pharmacy take reasonable precautions to ensure that only the minimum necessary amount of health information is disclosed?
- A. When the disclosure is to another covered entity for treatment purposes.
- B. When the disclosure is to a third party payer for payment purposes.
- C. When the disclosure is made for marketing purposes.
- D. All of the above.
8. Which of the following correctly describes what a pharmacy is required to do in order to guard against secondary, incidental disclosures of protected health information?
- A. A pharmacy must counsel patients only in a secure, sound-proof room designed specifically for counseling activities.

- B. A pharmacy must construct a sound-proof area to take telephone calls from doctors concerning a patient's medication needs or health conditions.
- C. A pharmacy must provide counseling only in written form.
- D. A pharmacy must take reasonable steps to ensure that protected health information is disclosed only to those persons who have a right to access the information.
9. Which of the following is included among the rights that a patient has with respect to his or her health information under HIPAA.
- A. The right to request copies of his or her records.
- B. The right to request amendments to the records.
- C. The right to obtain an accounting of disclosures of protected health information.
- D. All of the above.
10. Which of the following is correct concerning possible penalties for violations of the HIPAA privacy rules.
- A. Civil penalties can range from \$100 per violation, up to \$25,000 per person in any calendar year.
- B. Criminal penalties of up to \$50,000 and one year in jail are possible if a person knowingly discloses protected health information improperly.
- C. Covered entities can be fined up to \$250,000, and receive ten (10) years in jail, for using PHI for commercial advantage, personal gain or malicious harm.
- D. All of the above.

**Answer Key**

1. D.
2. A.
3. D.
4. B.
5. C.
6. D.
7. A.
8. D.
9. D.
10. D.