PeachtreeCE.com

Peachtree Professional Education, Inc.

(formerly FastCEUs.com)

Ethics 8
Privacy and Law

1 CE Hour

Peachtree Professional Education, Inc. is approved to provider continuing education services by the National Association of Alcohol and Drug Addiction Counselors (NAADAC) and the National Board of Certified Counselors (NBCC) as well as by many individual state regulatory boards for most mental health, and mental health nursing related professionals.

Peachtree Professional Education, Inc. has been approved by NBCC as an Approved Continuing Education Provider, ACEP No. 5701. Programs that do not qualify for NBCC credit are clearly identified. Peachtree Professional Education is solely responsible for all aspects of the programs.

Please see our main webpage at www.PeachtreeCE.com for a complete state-by-state and discipline listing of all our Board CE Provider Approvals, or contact your Board directly if you have course credit approval questions.

Peachtree Professional Education, Inc.
Dr.Richard K. Nongard, LMFT
15560 N. Frank L. Wright Blvd, #B4-118
Scottsdale, AZ 85260
Voice: (918) 236-6110

Please use the contact page on our website for a prompt email response:

www.PeachtreeCE.com

#8 Ethics: HIPAA, Privacy and Law

1 CE Credit Hours

Your instructor for this course is Dr. Richard K. Nongard, a Licensed Marriage and Family Therapist and the author of *Transformational Leadership: How to Lead form Your Strengths and Maximize your Impact* and *Contextual Psychology: Integrating Mindfulness-Based Approaches Into Effective Therapy.* His books can be found at any bookseller worldwide.

NOTE: This Peachtree Professional Education, Inc. online CE Course entails this packet of information, and also requires reading of your corresponding professional association's Code of Ethics. (External internet links are provided within this course material.)

Course Description:

This course discusses important information concerning patient privacy, electronic documentation, and information sharing regulations for client confidentiality.

Course Objectives:

At the conclusion of this course, the professional will be able to:

- Verbalize and understanding of their respective professional association's Code of Ethics.
- Apply a basic fundamentals of HIPAA law as it relates to practicing in the mental health industry.
- Provide client care consistent with ethical guideline and privacy considerations

Purpose of this course:

The purpose of this continuing education course is to provide a current understanding of issues relevant to the mental health counselor concerning new HIPPA guidelines for patient privacy. Current government facts, guidelines and information is provided to assist counselors in clarifying paperwork and electronic data concerns.

Course Outline:

Part 1: Reading of Your Corresponding Professional Association's Code of Ethics

Part 2: Reading of Course Introduction and Section 1: Patient Privacy

Part 3: Reading of Section 2: Common Questions and their Answers

Part 4: Administration and Completion of the Evaluation of Learning Quiz

==========

1 CE Credit Hour

Ethics #8

Privacy, Law and HIPAA

1 CE Credit Hour Course

Instructions for course completion:

1. The professional is required to read their respective professional association's Code of Ethics. (External web links are included on the following page.)

2. The professional is required to read the remaining course materials contained in this .pdf file.

3. Complete the required evaluation of learning quiz and return it to our office either online or by fax or mail, with the appropriate fee.

Each professional association has published a Code of Ethics. The National Association Of Social Workers, the American Association of Marriage And Family Therapists, The American Psychological Association, The National Association of Alcoholism and Drug Abuse Counselors and the American Counseling Association have all published Codes of Ethics unique to the professions that they serve. In addition, various states have published their own Codes of Ethics, applicable to licensed individuals in their state.

As part of this course, you are required to read your respective professional association's Code of Ethics. Most professionals will find a copy of the Code in their membership information packets.

For professionals who are licensed but not dues paying members of any professional association, please know that each professional association's website has their Code of Ethics published on the Internet, available for all to read.

From a liability perspective, it is important to note that whether we are a dues paying member or not of our respective professional association, in civil court we will be held to our professional association's ethical standards.

For example, if you are a Marriage and Family Therapist licensed by the state but not a member of the AAMFT, you will still be held to the ethical standards of the AAMFT for the services that you provide. If you are a Psychologist and not a dues paying member of the American Psychological Association, in civil court you will still be held to the ethical standards of your respective professional association's Code of Ethics.

When we face ethical dilemmas in our clinical practice, the answers to those dilemmas are often found in the basic principles of professional ethics provided by our professional associations.

The Codes of Ethics links below are provided for your convenience. Before or after you read the remaining course materials, please select the link for the association that corresponds to your professional licensure, and read their Code of Ethics. When you take the link - you will leave this document - you can use your browser's < back arrow to return, or you may wish to save this file in your Favorite Places. For most professions, the Code reading will be approximately 10-20 pages.

NOTE: Sometimes the Boards will move or change their links. If this happens, you can always find the new link to your Code by using an Internet Search Engine, like www.google.com.

NAADAC - National Association of Alcohol and Drug Abuse Counselors

http://www.naadac.org/assets/1959/naadac_code_of_ethics_brochure.pdf

NBCC - National Board of Certified Counselors

http://www.nbcc.org/Assets/Ethics/NBCCCodeofEthics.pdf

APA - American Psychological Association

http://www.apa.org/ethics/

ACA - American Counseling Association

https://www.counseling.org/resources/aca-code-of-ethics.pdf

AAMFT - American Association of Marriage and Family Therapists

https://www.aamft.org/iMIS15/AAMFT/Content/legal_ethics/code_of_ethics.aspx

NASW - National Association of Social Workers

http://www.socialworkers.org/pubs/code/default.asp

SECTION 1

PROTECTING THE PRIVACY OF PATIENTS' HEALTH INFORMATION

Overview:

The first-ever federal privacy standards to protect patients' medical records and other health information provided to health plans, doctors, hospitals and other health care providers took effect on April 14, 2003. Developed by the Department of Health and Human Services (HHS), these new standards provide patients with access to their medical records and more control over how their personal health information is used and disclosed. They represent a uniform, federal floor of privacy protections for consumers across the country. State laws providing additional protections to consumers are not affected by this new rule.

Congress called on HHS to issue patient privacy protections as part of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). HIPAA included provisions designed to encourage electronic transactions and also required new safeguards to protect the security and confidentiality of health information. The final regulation covers health plans, health care clearinghouses, and those health care providers who conduct certain financial and administrative transactions (e.g., enrollment, billing and eligibility verification) electronically. Most health insurers, pharmacies, doctors and other health care providers were required to comply with these federal standards beginning April 14, 2003. As provided by Congress, certain small health plans have an additional year to comply. HHS has conducted extensive outreach and provided guidance and technical assistant to these providers and businesses to make it as easy as possible for them to implement the new privacy protections. These efforts include answers to hundreds of common questions about the rule, as well as explanations and descriptions about key elements of the rule.

These materials are available at http://www.hhs.gov/ocr/hipaa.

PATIENT PROTECTIONS

The new privacy regulations ensure a national floor of privacy protections for patients by limiting the ways that health plans, pharmacies, hospitals and other covered entities can use patients' personal medical information. The regulations protect medical records and other individually identifiable health information, whether it is on paper, in computers or communicated orally. Key provisions of these new standards include:

Access to Medical Records. Patients generally should be able to see and obtain copies of their medical records and request corrections if they identify errors and mistakes. Health plans, doctors, hospitals, clinics, nursing homes and other covered entities generally should provide access these records within 30 days and may charge patients for the cost of copying and sending the records.

Notice of Privacy Practices. Covered health plans, doctors and other health care providers must provide a notice to their patients how they may use personal medical information and their rights under the new privacy regulation. Doctors, hospitals and other direct-care providers generally will provide the notice on the patient's first visit following the April 14, 2003, compliance date and upon request. Patients generally will be asked to sign, initial or otherwise acknowledge that they received this notice. Health plans generally must mail the notice to their enrollees by April 14 and again if the notice changes significantly. Patients also may ask covered entities to restrict the use or disclosure of their information beyond the practices included in the notice, but the covered entities would not have to agree to the changes.

Limits on Use of Personal Medical Information. The privacy rule sets limits on how health plans and covered providers may use individually identifiable health information. To promote the best quality care for patients, the rule does not restrict the ability of doctors, nurses and other providers to share information needed to treat their patients. In other situations, though, personal health information generally may not be used for purposes not related to health care, and covered entities may use or share only the minimum amount of protected information needed for a particular purpose. In addition, patients would have to sign a specific

authorization before a covered entity could release their medical information to a life insurer, a bank, a marketing firm or another outside business for purposes not related to their health care.

Prohibition on Marketing. The final privacy rule sets new restrictions and limits on the use of patient information for marketing purposes. Pharmacies, health plans and other covered entities must first obtain an individual's specific authorization before disclosing their patient information for marketing. At the same time, the rule permits doctors and other covered entities to communicate freely with patients about treatment options and other health-related information, including disease-management programs.

Stronger State Laws. The new federal privacy standards do not affect state laws that provide additional privacy protections for patients. The confidentiality protections are cumulative; the privacy rule will set a national "floor" of privacy standards that protect all Americans, and any state law providing additional protections would continue to apply. When a state law requires a certain disclosure -- such as reporting an infectious disease outbreak to the public health authorities -- the federal privacy regulations would not preempt the state law.

Confidential communications. Under the privacy rule, patients can request that their doctors, health plans and other covered entities take reasonable steps to ensure that their communications with the patient are confidential. For example, a patient could ask a doctor to call his or her office rather than home, and the doctor's office should comply with that request if it can be reasonably accommodated.

Complaints. Consumers may file a formal complaint regarding the privacy practices of a covered health plan or provider. Such complaints can be made directly to the covered provider or health plan or to HHS' Office for Civil Rights (OCR), which is charged with investigating complaints and enforcing the privacy regulation. Information about filing complaints should be included in each covered entity's notice of privacy practices. Consumers can find out more information about filing a complaint at http://www.hhs.gov/ocr/hipaa or by calling (866) 627-7748.

HEALTH PLANS AND PROVIDERS

The privacy rule requires health plans, pharmacies, doctors and other covered entities to establish policies and procedures to protect the confidentiality of protected health information about their patients. These requirements are flexible and scalable to allow different covered entities to implement them as appropriate for their businesses or practices. Covered entities must provide all the protections for patients cited above, such as providing a notice of their privacy practices and limiting the use and disclosure of information as required under the rule. In addition, covered entities must take some additional steps to protect patient privacy:

Written Privacy Procedures. The rule requires covered entities to have written privacy procedures, including a description of staff that has access to protected information, how it will be used and when it may be disclosed. Covered entities generally must take steps to ensure that any business associates who have access to protected information agree to the same limitations on the use and disclosure of that information.

Employee Training and Privacy Officer. Covered entities must train their employees in their privacy procedures and must designate an individual to be responsible for ensuring the procedures are followed. If covered entities learn an employee failed to follow these procedures, they must take appropriate disciplinary action.

Public Responsibilities. In limited circumstances, the final rule permits -- but does not require --covered entities to continue certain existing disclosures of health information for specific public responsibilities. These permitted disclosures include: emergency circumstances; identification of the body of a deceased person, or the cause of death; public health needs; research that involves limited data or has been independently approved by an Institutional Review Board or privacy board; oversight of the health care system; judicial and administrative proceedings; limited law enforcement activities; and activities related to national defense and security. The privacy rule generally establishes new safeguards and limits on these disclosures. Where no other law requires disclosures in these situations, covered entities may continue to use their professional judgment to decide whether to make such disclosures based on their own policies and ethical principles.

Equivalent Requirements For Government. The provisions of the final rule generally apply equally to private sector and public sector covered entities. For example, private hospitals and government-run hospitals covered by the rule have to comply with the full range of requirements.

OUTREACH AND ENFORCEMENT

HHS' Office for Civil Rights (OCR) oversees and enforces the new federal privacy regulations. Led by OCR, HHS has issued extensive guidance and technical assistance materials to make it as easy as possible for covered entities to comply with the new requirements. Key elements of OCR's outreach and enforcement efforts include:

Guidance and technical assistance materials. HHS has issued extensive guidance and technical materials to explain the privacy rule, including an extensive, searchable collection of frequently asked questions that address major aspects of the rule. HHS will continue to expand and update these materials to further assist covered entities in complying. These materials are available at http://www.hhs.gov/ocr/hipaa/assist.html.

Conferences and seminars. HHS has participated in hundreds of conferences, trade association meetings and conference calls to explain and clarify the provisions of the privacy regulation. These included a series of regional conferences sponsored by HHS, as well as many held by professional associations and trade groups. HHS will continue these outreach efforts to encourage compliance with the privacy requirements.

Information line. To help covered entities find out information about the privacy regulation and other administrative simplification provisions of the Health Insurance Portability and Accountability Act of 1996, OCR and HHS' Centers for Medicare & Medicaid Services have established a toll-free information line. The number is (866) 627-7748.

Complaint investigations. Enforcement will be primarily complaint-driven. OCR will investigate complaints and work to make sure that consumers receive the privacy rights and protections required under the new regulations. When appropriate, OCR can impose civil monetary penalties for violations of the privacy rule provisions. Potential criminal

violations of the law would be referred to the U.S. Department of Justice for further investigation and appropriate action.

Civil and Criminal Penalties. Congress provided civil and criminal penalties for covered entities that misuse personal health information. For civil violations of the standards, OCR may impose monetary penalties up to $100 per violation, up to $25,000 per year, for each requirement or prohibition violated. Criminal penalties apply for certain actions such as knowingly obtaining protected health information in violation of the law. Criminal penalties can range up to $50,000 and one year in prison for certain offenses; up to $100,000 and up to five years in prison if the offenses are committed under "false pretenses"; and up to $250,000 and up to 10 years in prison if the offenses are committed with the intent to sell, transfer or use protected health information for commercial advantage, personal gain or malicious harm.

SECTION 2

COMMON HIPAA QUESTIONS AND THEIR ANSWERS

Question: Generally, what does the HIPAA Privacy Rule require the average provider or health plan to do?

Answer:
For the average health care provider or health plan, the Privacy Rule requires activities, such as:

- Notifying patients about their privacy rights and how their information can be used.

- Adopting and implementing privacy procedures for its practice, hospital, or plan.

- Training employees so that they understand the privacy procedures.

- Designating an individual to be responsible for seeing that the privacy procedures are adopted and followed.

- Securing patient records containing individually identifiable health information so that they are not readily available to those who do not need them.

Responsible health care providers and businesses already take many of the kinds of steps required by the Rule to protect patients' privacy. Covered entities of all types and sizes are required to comply with the Privacy Rule. To ease the burden of complying with the new requirements, the Privacy Rule gives needed flexibility for providers and plans to create their own privacy procedures, tailored to fit their size and needs. The scalability of the Rule provides a more efficient and appropriate means of safeguarding protected health information than would any single standard. For example,

- The privacy official at a small physician practice may be the office manager, who will have other non-privacy related duties; the privacy official at a large health plan may be a full-time position, and may have the regular support and advice of a privacy staff or board.

- The training requirement may be satisfied by a small physician practice's providing each new member of the workforce with a copy of its privacy policies and documenting that new members have reviewed the policies; whereas a large health plan may provide training through live instruction, video presentations, or interactive software programs.

- The policies and procedures of small providers may be more limited under the Rule than those of a large hospital or health plan, based on the volume of health information maintained and the number of interactions with those within and outside of the health care system.

Question

Who must comply with these new HIPAA privacy standards?

Answer

As required by Congress in HIPAA, the Privacy Rule covers:

- Health plans

- Health care clearinghouses

- Health care providers who conduct certain financial and administrative transactions electronically. These electronic transactions are those for which standards have been adopted by the Secretary under HIPAA, such as electronic billing and fund transfers.

These entities (collectively called "covered entities") are bound by the new privacy standards even if they contract with others (called "business associates") to perform some of their essential functions. The law does not give the Department of Health and Human Services (HHS) the authority to regulate other types of private businesses or public agencies through this regulation. For example, HHS does not have the authority to regulate employers, life insurance companies, or public agencies that deliver social security or welfare benefits. See the fact sheet and frequently asked questions on this web site about the standards on "Business Associates" for a more detailed discussion of the covered entities' responsibilities when they engage others to perform essential functions or services for them.

Question

Does the HIPAA Privacy Rule allow parents the right to see their children's medical records?

Answer

Yes, the Privacy Rule generally allows a parent to have access to the medical records about his or her child, as his or her minor child's personal representative when such access is not inconsistent with State or other law.

There are three situations when the parent would not be the minor's personal representative under the Privacy Rule. These exceptions are: (1) when the minor is the one who consents to care and the consent of the parent is not required under State or other applicable law; (2) when the minor obtains care at the direction of a court or a person appointed by the court; and (3) when, and to the extent that, the parent agrees that the minor and the health care provider may have a confidential relationship. However, even in these exceptional situations, the parent may have access to the medical records of the minor related to this treatment when State or other applicable law requires or permits such parental access. Parental access would be denied when State or other law prohibits such access. If State or other applicable law is silent on a parent's right of access in these cases, the licensed health care provider may exercise his or her professional judgment to the extent allowed by law to grant or deny parental access to the minor's medical information.

Finally, as is the case with respect to all personal representatives under the Privacy Rule, a provider may choose not to treat a parent as a personal representative when the provider reasonably believes, in his or her professional judgment, that the child has been or may be subjected to domestic violence, abuse or neglect, or that treating the parent as the child's personal representative could endanger the child.

Question

Can a physician's office FAX patient medical information to another physician's office?

Answer

The HIPAA Privacy Rule permits physicians to disclose protected health information to another health care provider for treatment purposes. This can be done by fax or by other means.

Covered entities must have in place reasonable and appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information that is disclosed using a fax machine. Examples of measures that could be reasonable and appropriate in such a situation include the sender confirming that the fax number to be used is in fact the correct one for the other physician's office, and placing the fax machine in a secure location to prevent unauthorized access to the information. See 45 CFR164.530(c).

Question

Does the HIPAA Privacy Rule strictly prohibit the use, disclosure, or request of an entire medical record? If not, are case-by-case justifications required each time the entire medical record is disclosed?

Answer

No. The Privacy Rule does not prohibit the use, disclosure, or request of an entire medical record; and a covered entity may use, disclose, or request an entire medical record without a case-by-case justification, if the covered entity has documented in its policies and procedures that the entire medical record is the amount reasonably necessary for certain identified purposes. For uses, the policies and procedures would identify those persons or classes of person in the workforce that need to see the entire medical record and the conditions, if any, that are appropriate for such access. Policies and procedures for routine disclosures and requests and the criteria used for non-routine disclosures and requests would identify the circumstances under which disclosing or requesting the entire medical record is reasonably necessary for particular purposes.

The Privacy Rule does not require that a justification be provided with respect to each distinct medical record.

Finally, no justification is needed in those instances where the minimum necessary standard does not apply, such as disclosures to or requests by a health care provider for treatment purposes or disclosures to the individual who is the subject of the protected health information.

Question

A provider might have a patient's medical record that contains older portions of a medical record that were created by another previous provider. Will the HIPAA Privacy Rule permit a provider who is a covered entity to disclose a complete medical record even though portions of the record were created by other providers?

Answer

Yes, the Privacy Rule permits a provider who is a covered entity to disclose a complete medical record including portions that were created by another provider, assuming that the disclosure is for a purpose permitted by the Privacy Rule, such as treatment.

Question

What is the difference between “consent” and “authorization” under the HIPAA Privacy Rule?

Answer

The Privacy Rule permits, but does not require, a covered entity voluntarily to obtain patient consent for uses and disclosures of protected health information for treatment, payment, and health care operations. Covered entities that do so have complete discretion to design a process that best suits their needs.

By contrast, an “authorization” is required by the Privacy Rule for uses and disclosures of protected health information not otherwise allowed by the Rule. Where the Privacy Rule requires patient authorization, voluntary consent is not sufficient to permit a use or disclosure of protected health information unless it also satisfies the requirements of a valid authorization. An authorization is a detailed document that gives covered entities permission to use protected health information for specified purposes, which are generally other than treatment, payment, or health care operations, or to disclose protected health information to a third party specified by the individual. An authorization must specify a number of elements, including a description of the protected health information to be used and disclosed, the person authorized to make the use or disclosure, the person to whom the covered entity may make the disclosure, an expiration date, and, in some cases, the purpose for which the information may be used or disclosed. With limited exceptions, covered entities may not condition treatment or coverage on the individual providing an authorization.

Question

Are the following types of insurance covered under HIPAA: long/short term disability; workers' compensation; automobile liability that includes coverage for medical payments?

Answer

No, the listed types of policies are not health plans. The HIPAA Administrative Simplification regulations specifically exclude from the definition of a "health plan" any policy, plan, or program to the extent that it provides, or pays for the cost of, excepted benefits, which are listed in section 2791(c)(1) of the Public Health Service Act, 42 U.S.C. 300gg-91(c)(1). See 45 CFR 160.103. As described in the statute, excepted benefits are one or more (or any combination thereof) of the following policies, plans or programs:

- Coverage only for accident, or disability income insurance, or any combination thereof.

- Coverage issued as a supplement to liability insurance.
- Liability insurance, including general liability insurance and automobile liability insurance.

- Workers' compensation or similar insurance.

- Automobile medical payment insurance.

- Credit-only insurance.

- Coverage for on-site medical clinics

- Other similar insurance coverage, specified in regulations, under which benefits for medical care are secondary or incidental to other insurance benefits.

Question

A clinic customarily places patient charts in the plastic box outside an exam room. It does not want the record left unattended with the patient, and physicians want the record close by for fast review right before they walk into the exam room. Will the HIPAA Privacy Rule allow the clinic to continue this practice?

Answer

Yes, the Privacy Rule permits this practice as long as the clinic takes reasonable and appropriate measures to protect the patient's privacy. The physician or other health care professionals use the patient charts for treatment purposes. Incidental disclosures to others that might occur as a result of the charts being left in the box are permitted, if the minimum necessary and reasonable safeguards requirements are met. See 45 CFR 164.502(a)(1)(iii). As the purpose of leaving the chart in the box is to provide the physician with access to the medical information relevant to the examination, the minimum necessary requirement would be satisfied. Examples of measures that could be reasonable and appropriate to safeguard the patient chart in such a situation would be limiting access to certain areas, ensuring that the area is supervised, escorting non-employees in the area, or placing the patient chart in the box with the front cover facing the wall rather than having protected health information about the patient visible to anyone who walks by. Each covered entity must evaluate what measures are reasonable and appropriate in its environment. Covered entities may tailor measures to their particular circumstances.

Question

Does a physician need a patient's written authorization to send a copy of the patient's medical record to a specialist or other health care provider who will treat the patient?

Answer

No. The HIPAA Privacy Rule permits a health care provider to disclose protected health information about an individual, without the individual's authorization, to another health care provider for that provider's treatment of the individual. See 45 CFR 164.506 and the definition of "treatment" at 45 CFR 164.501.

Question

When is a health care provider a business associate of another health care provider?

Answer

The HIPAA Privacy Rule explicitly excludes from the business associate requirements disclosures by a covered entity to a health care provider for treatment purposes. See 45 CFR 164.502(e)(1). Therefore, any covered health care provider (or other covered entity) may share protected health information with a health care provider for treatment purposes without a business associate contract. However, this exception does not preclude one health care provider from establishing a business associate relationship with another health care provider for some other purpose. For example, a hospital may enlist the services of another health care provider to assist in the hospital's training of medical students. In this case, a business associate contract would be required before the hospital could allow the health care provider access to patient health information.

Question

If patients request copies of their medical records as permitted by the Privacy Rule, are they required to pay for the copies?

Answer

The Privacy Rule permits the covered entity to impose reasonable, cost-based fees. The fee may include only the cost of copying (including supplies and labor) and postage, if the patient requests that the copy be mailed. If the patient has agreed to receive a summary or explanation of his or her protected health information, the covered entity may also charge a fee for preparation of the summary or explanation. The fee may not include costs associated with searching for and retrieving the requested information. See 45 CFR 164.524.

Question

Does the HIPAA Privacy Rule require hospitals and doctors' offices to be retrofitted, to provide private rooms, and soundproof walls to avoid any possibility that a conversation is overheard?

Answer

No, the Privacy Rule does not require these types of structural changes be made to facilities.

Covered entities must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information. This standard requires that covered entities make reasonable efforts to prevent uses and disclosures not permitted by the Rule. The Department does not consider facility restructuring to be a requirement under this standard.

For example, the Privacy Rule does not require the following types of structural or systems changes:

- Private rooms.

- Soundproofing of rooms.

- Encryption of wireless or other emergency medical radio communications which can be intercepted by scanners.

- Encryption of telephone systems.

Covered entities must implement reasonable safeguards to limit incidental, and avoid prohibited, uses and disclosures. The Privacy Rule does not require that all risk of protected health information disclosure be eliminated. Covered entities must review their own practices and determine what steps are reasonable to safeguard their patient information. In determining what is reasonable, covered entities should assess potential risks to patient privacy, as well as consider such issues as the potential effects on patient care, and any administrative or financial burden to be incurred from implementing particular safeguards. Covered entities also may take into consideration the steps that other prudent health care and health information professionals are taking to protect patient privacy.

Examples of the types of adjustments or modifications to facilities or systems that may constitute reasonable safeguards are:

- Pharmacies could ask waiting customers to stand a few feet back from a counter used for patient counseling.

- In an area where multiple patient-staff communications routinely occur, use of cubicles, dividers, shields, curtains, or similar barriers may constitute a reasonable safeguard. For example, a large clinic intake area may reasonably use cubicles

Course Conclusion

Instructions for earning continuing education hours:

Thank you for taking this course.

All quizzes are now online at www.PeachtreeCE.com

We no longer support submission through mail, fax or email. You must use a credit card to complete payment for this course.

If you have any questions, email our office at: Richard@PeachtreeCE.com