An Overview of HIPAA for Healthcare Professionals

This course has been awarded one (1.0) contact hour.
This course expires on September 29, 2015.

This program has been pre-approved by The Commission for Case Manager Certification to provide continuing education credit to CCM® board certified case managers. The course is approved for **1 clock hour**. Activity code: W0000081. Approval Number: 20130781.

First Published: September 29, 2009
Updated: September 29, 2012

Acknowledgements

RN.com acknowledges the valuable contributions of…

…Nadine Salmon, MSN, BSN, IBCLC is the Clinical Content Specialist for RN.com. She is a South African trained Registered Nurse, Midwife and International Board Certified Lactation Consultant. Nadine obtained an MSN at Grand Canyon University, with an emphasis on Nursing Leadership. Her clinical background is in Labor & Delivery and Postpartum nursing, and she has also worked in Medical Surgical Nursing and Home Health. Nadine has work experience in three countries, including the United States, the United Kingdom and South Africa. She worked for the international nurse division of American Mobile Healthcare, prior to joining the Education Team at RN.com. Nadine is a nurse planner for RN.com and is responsible for all clinical aspects of course development. She updates course content to current standards, and develops new course materials for RN.com.

…Amy Ginter and Karen Siroky, contributing authors of this course.

Purpose and Objectives

The purpose of An Overview of HIPAA for Healthcare Professionals is to provide you with information about the HIPAA law and its guidelines. This course covers various aspects of confidentiality, communication, record keeping and how it applies in caring for patients. The course also contains useful information about how to manage encounters with Protected Health Information (PHI) in relation to HIPAA and compliance.

After successful completion of this course, the healthcare professional will be able to:

1. Describe what HIPAA is and what portion of the law was recently enacted.
2. Identify who is obligated to maintain patient confidentiality.
3. Identify what type of patient communication and information sharing requires compliance under HIPAA.
4. Describe what PHI is and why it is important.
5. Define 'Notice of Privacy Practices' and 'Minimum Necessary Standard'.
6. Describe the penalties for non-compliance with HIPAA requirements.

Introduction

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 was developed to protect patients' rights and confidentiality in a healthcare environment that is becoming increasingly more technologically advanced. These guidelines apply in every healthcare setting and to every patient. They refer to the sharing of all communications between other providers, families, friends and the media. A working knowledge of the HIPAA law will assist you in understanding your role in maintaining the confidentiality of your patient's medical information.

HIPAA was enacted to cover three specific areas:

1. Insurance portability or the ability to move to another employer and be certain that insurance coverage will not be denied
2. Fraud enforcement and accountability
3. Administrative simplification

Insurance portability and fraud enforcement and accountability have been active since 1996; however, it took until April 2003 to enact administrative simplification.

In January 2013, further amendments were made to HIPAA law, to further protect patient privacy, secure health information and enhance standards to improve privacy protections and security safeguards for consumer health data.

The final omnibus rule greatly enhances a patient's privacy protections, provides individuals new rights to their health information, and strengthens the government's ability to enforce the law.

Administrative simplification refers to the guidelines that impact healthcare providers in the communications with other providers, families, friends and the media.

The overall intent of this act is to make it easier for the consumer to obtain seamless care, irrespective of the number of different providers they see; while still protecting the confidentiality and privacy of the patient.

Covered Entities

HIPAA's privacy and security provisions apply to 'covered entities.' A covered entity is any healthcare organization (including a healthcare clearinghouse and health plan) that conducts the transaction of

confidential medical information in electronic form. This term applies to all members of the workforce of a healthcare organization. This includes all employees, such as nurses, pharmacists, physicians and administrative, clerical, food service and environmental services staff. The adherence to HIPAA policies also applies to volunteers and any other personnel under the facility's direct supervision.

In addition, HIPAA states that "Business Associates" who may be independent contractors or separate service providers must also comply with HIPAA security provisions. These may include:

- Outsourced retail service providers, such as baby photographers
- Outside laboratory or imaging services
- Outside computer technicians
- Accreditation agencies that may need to review patient information during a survey.

Your organization may have different arrangements with various service providers. Ensure that you are familiar with the service providers for your particular organization.

A 'covered entity' is any person, business or institution that provides healthcare or keeps medical records on patients. All healthcare professionals who have direct relationships with patients are considered "covered entities" and must comply with HIPAA laws.

***Test Yourself*: HIPAA's privacy and security provisions apply to the following members of the workforce of a facility: Pharmacists, Clerical staff, Nurses, or <u>All workforce members</u>**

Changes in Law Relating To Covered Entities

In January 2013, changes to the HIPAA law were made that expand many of the requirements to business associates of covered entities that receive protected health information, such as contractors and subcontractors.

Some of the largest breaches reported to Human Health Services have involved business associates.

Penalties are increased for noncompliance based on the level of negligence with a maximum penalty of $1.5 million per violation.

These changes also strengthen the Health Information Technology for Economic and Clinical Health (HITECH) Breach Notification requirements by clarifying when breaches of unsecured health information must be reported to HHS.

The HIPAA Privacy and Security Rules have focused on health care providers, health plans and other entities that process health insurance claims.

Amendments to the final rule, passed in January 2013, gives covered entities and business associates up to one year after the 180-day compliance date to modify contracts to comply with the new provisions of the rule.

Protected Health Information

The term Protected Health Information (PHI) is a term that you might hear frequently in the organization in which you work. PHI refers to personal patient information that can be used to identify the patient, sometimes even inadvertently. Patients have the right to direct when, why and to whom PHI may be released.

In the past, aggregated patient information may have been collected for research, quality improvement or other purposes. Even though the patient's name would be omitted, the patient may still be identifiable through specific data including date of procedure, type of procedure, gender or any number of other details. HIPAA allows patients much more control over PHI.

In January 2013, a change in the HIPAA Law provides the public with increased protection and control of personal health information. The final rule also streamlines an individual's ability to authorize the use of their health information for research purposes.

HIPAA guarantees patients rights to inspect their own medical records, correct errors, inquire who has access to their records and seek penalties if their medical information has been used inappropriately.

PHI is any information transmitted and / or maintained in any form, including prescription records, billing information, patient profiles and oral communications on the phone or during counseling.

Privacy Verses Confidentiality

HIPAA requires healthcare professionals to maintain the privacy and confidentiality of all PHI.

Privacy is the individual's right to decide who, when and how information about him or herself is disclosed.

Confidentiality is the obligation of another to maintain the person's privacy.

Although every facility has to comply with HIPAA, there is some flexibility in the methods used by each facility.

Under the new law, individual rights are expanded in important ways. Patients can ask for a copy of their electronic medical record in an electronic form. When individuals pay by cash they can instruct their provider not to share information about their treatment with their health plan.

The final omnibus rule sets new limits on how information is used and disclosed for marketing and fundraising purposes and prohibits the sale of an individuals' health information without their permission.

***Test Yourself*: Privacy is defined as the obligation of another to maintain the person's privacy. – False, *Confidentiality* is the obligation of another to maintain the person's privacy.**

Consents and Authorizations

Upon entering a healthcare organization, the patient is given information about how the organization will protect the privacy of the patient and what types of information will be shared and under what circumstances (generally related to the current care of the patient). This is called the Notice of Privacy Practices and is required by HIPAA to be given to all patients.

Under HIPAA, a facility may share or disclose patient information for the following purposes:

- Treatment of the patient (e.g. consulting with other healthcare providers on diagnosis and treatment)
- Obtaining payment from the patient's health plan
- Operational requirements (e.g. quality improvement activities or peer review)
- Complying with legally mandated reporting or disclosure

The patient must provide consent or further authorize any other release of information for any other purpose.

The organization must also make a good faith effort to obtain a written acknowledgement that the patient received the Privacy Notice.

***Did you know*? Under the new law, it is easier for parents and others to give permission to share proof of a child's immunization with a school.**

Notice of Privacy Practices

Every patient must be given a "Notice of Privacy Practice" (NPP) document. This describes to the patient how the organization will use and disclose their medical record information. The patient signs that they have received a copy of this notice. This notice is given once only, and a single privacy notice covers all pharmacies in a chain or all departments in a hospital. If the patient is unable to sign the NPP, the reason is documented. If signed by another person, the relationship of the person signing is documented as well.

This Notice of Privacy Practices essentially replaces the patient's signed consent. Once a Notice of Privacy Practices has been received and signed by the patient, it is no longer necessary for a healthcare professional to obtain additional consents or authorizations for any disclosures of PHI in the normal course of events.

If the patient does have any additional privacy requests, they should be documented on the privacy notice at the time of initial signing. For example, a patient may request that no-one other than the patient may pick up a prescription; or require that hospital staff do not discuss his medical condition with family or friends. Healthcare professionals should document these requests in the patient's records.

Since the Notice of Privacy Practices has essentially replaced the need for a patient's signed consent, prescriptions can now be received by a pharmacist without prior consent of a patient. Consent is now optional.

Patient Rights

Patient rights related to HIPAA include the right to receive the previously described Notice of Privacy Practices. Patients also have a right to request restrictions on the information shared as long as it is not related to the course of treatment. Patients can specify where and how communication of confidential information is handled, for instance specify a work number instead of a home number for messages.

Patients have the right to inspect, review and receive a copy of their PHI. Patients may also request an amendment or change in the content of the PHI if they believe there is an error or have another concern about the contents of the record. The provider has the right to accept or deny this request.

Every patient has the right to request and to receive an accounting of disclosures made of his PHI. While most PHI disclosures are subject to an accounting, there are some disclosures that are not required to be included; for instance, when shared with practitioners participating in treatment. If a patient believes that their privacy has been violated, it should be reported to the Office of Civil Rights. Refer to your facility's specific policy for detailed information on all issues about patient rights and HIPAA.

What Kind of Information is Protected?

Patient information that is protected includes, but is not limited to, the patient's name, address, telephone number, age, diagnosis, surgery, date of procedure and medications. Beyond this, additional information that

is protected includes any medical history information, results of physical examinations, laboratory and other diagnostic results, billing records and claim forms. Any information that could be used to identify the patient is protected under HIPAA.

It is important to know that this information is protected in any form, be it written, electronic or verbal.

Minimum Necessary Concept:

HIPAA demands that HIPAA limits use and disclosure of personal health information to a "minimum necessary" standard for any communications other than the purpose of treatment. This ensures that patient privacy will be protected by disclosing only the least amount of information necessary for another healthcare professional to perform their job. Thus, a Pharmacy Technician or Nursing Assistant (CNA) may need access to some information to allow them to fulfill their duties, but do not need access to full medical records.

Patient Directory

Every organization maintains a patient directory that lists patient names, room numbers (if applicable) and condition. This information can be provided to anyone who asks about a particular patient.

Patients can request to be excluded from this directory, and then no information is released. There is also a written notice that allows a patient to limit the disclosure of information to next of kin. If this option is enacted, it is documented in the medical record. Certain diagnoses are also excluded from this standard, and therefore no information is released.

An organization may opt not to have a directory and a patient may opt NOT to be included in the directory. A patient's medical diagnosis is never disclosed.

In either of these circumstances, the response to requests for patient information would be "I have no information on anyone with that name" or a similar neutral statement that neither confirms nor denies any information.

How Does HIPAA Affect Discussion of Patient Issues?

Although there are persons with whom you need to communicate about a specific patient, be certain to consider the following:

- Does the person you are communicating with "need to know" the information about the patient? In other words, is there a medical necessity to discuss the patient?
- Are you discussing the patient out of the hearing of others?
- Without using a patient name, are you still discussing the patient in a way that others could discern who you are speaking about? For example, perhaps there is only one male on your unit, so if you use the word "he," others will know who you are discussing. In a retail pharmacy setting, pharmacists need to exercise additional discretion when talking on the phone or counseling a patient on his medications in a public setting.

HIPAA requires healthcare professionals to make their best efforts to protect patient's privacy by sharing the least amount of information necessary to provide care.

Discussing Patient Information with Family and Personal Representatives

A personal representative is defined as any person who is legally authorized to act on behalf of the patient. This can be someone with a legal document, such as a general power of attorney or a more limited medical power of attorney or simply someone who has the authority to act on behalf of the patient. PHI can be shared with a personal representative.

HIPAA allows disclosure of PHI to spouses, parents, legal guardians and others involved in a patient's care without obtaining the patient's formal, written permission. If you need to discuss a particular care plan or course of treatment with a patient when others are present, simply ask the patient if there is any objection.

***Test Yourself*: A personal representative is defined as any person who: Is related to the patient, Who can identify and knows where the patient resides, Is a physician, or Someone with a legal document or who has the authority to act on behalf of the patient.**

Using and Sharing Information

Most likely, all the personal information that you use and share in your daily duties is covered under HIPAA for "treatment" purposes. These include:

- Discussing diagnosis and treatment with other healthcare professionals.
- Performing diagnostic tests and providing this information to other providers.
- Providing laboratory samples or imaging tests to those who perform diagnostics on them.
- Referring a patient to another provider or facility, and discussing the treatment and/or diagnosis.
- Telephone prescription information to a pharmacy.

For treatment purposes, you are not limited by HIPAA in terms of the information you can provide to other providers or caregivers, as long as the patient has not requested to restrict the sharing of his or her information. If this were the case, a patient's record would reflect this request.

While "treatment purposes" allows you a broader scope for sharing information, you will still want to be aware of "the need to know" standard. For example, the Pharmacy Technician delivering medications does not need to know details of the patients' illness beyond those that would affect the delivery of that medication.

Disclosure of PHI is allowed provided that the other healthcare professional has a direct treatment relationship with the patient, and has informed the patient of their own privacy policy.

Since the inception of HIPAA, many healthcare providers are concerned about engaging in confidential conversations with other providers or with patients if there is a possibility that they could be overheard. The HIPAA Privacy Rule is not intended to prohibit providers from talking to each other and to their patients. Provisions of this Rule requiring covered entities to implement reasonable safeguards to ensure that providers' primary consideration is the appropriate treatment of their patients. The Privacy Rule recognizes that oral communications often must occur freely and quickly in treatment settings. Thus, covered entities are free to engage in communications as required. The Privacy Rule also recognizes that overheard communications in these settings may be unavoidable and allows for these incidental disclosures.

The following practices are permissible under the Privacy Rule, if reasonable precautions are taken to minimize the chance of incidental disclosures to others who may be nearby:

- Healthcare staff may orally coordinate services at hospital nursing stations.
- Nurses or other healthcare professionals may discuss a patient's condition over the phone with the

patient, a provider or a family member.
- Healthcare professionals may discuss a patient's condition during training rounds in an academic or training institution.
- A pharmacist may discuss a prescription with a patient or physician over the phone.

In an emergency situation, the law allows covered entities to engage in communications as required for quick, effective and high quality healthcare.

HIPAA Violations Verses Acceptable Practice

As a healthcare provider, it is extremely important to be aware of HIPAA laws and the need to protect a patient's privacy in the clinical setting. The following examples illustrate every day, common situations in which healthcare professionals may inadvertently and unintentionally violate a patient's privacy in the course of performing daily activities.

Identify which of the following situations violate HIPAA privacy laws and which of the situations are acceptable practices:

- Nurse Johns tells the baby photographer "mom decided to have her tubes tied after having this little guy."

Is this a Violation or Acceptable Practice? – **Violation**: The Baby Photographer does not need to know that the mother intends to have a tubal ligation.

- Clergy member tells physical therapist "Mr. Jones is worried about what happens to his soul after he dies."

Is this a Violation or Acceptable Practice? – **Violation**: The PT does not need this additional information n order to perform his duties. This is an unnecessary breach of confidentiality.

- Pharmacist calls out "Mr. Gregory, your prescription is ready."

Is this a Violation or Acceptable Practice? – **Acceptable Practice**: The pharmacist is respecting the confidentiality of the patient by not announcing what the prescription is for.

- Pharmacy Technician calls out "Ms. Smith, your blood pressure medicine is ready."

Is this a Violation or Acceptable Practice? – **Violation**: There was no need to announce that the prescription was for antihypertensive medication. This is a violation of the patient's privacy.

- Nurse tells pharmacist "Mr. Jones says he doesn't take all his meds at home as they are difficult to swallow."

Is this a Violation or Acceptable Practice? – **Acceptable Practice**: This is important information for the pharmacist to have, in order to ensure that the patient's needs are met.

- The respiratory therapist tells the nurse "Mr. James seems to have given up. I am really worried about him."

Is this a Violation or Acceptable Practice? – **Acceptable Practice**: It is important for healthcare professionals to share relevant observations about a patient so that care can be coordinated and focused on the patient's needs.

Sign-in Sheets and Calls to Home

Patients have become very aware of HIPAA due to changes in policy regarding:

- Sign-in sheets in waiting rooms or retail pharmacy stores
- Calling out a patient's name in a public area (waiting room or retail pharmacy)
- Leaving a message on a home message machine
- Leaving a message with a relative at a home number

However, HIPAA has specific features to allow these to continue.

Facilities may continue to use patient sign-in sheets or call out patient names in waiting rooms, as long as the information disclosed is appropriately limited. However, these incidental disclosures are permitted only when the covered entity has implemented reasonable safeguards and the minimum necessary standard, where appropriate. For example, the sign-in sheet may not display medical information that is not necessary for the purpose of signing in (e.g., the medical problem for which the patient is seeing the physician, or the condition for which the medication is being prescribed) (U.S. Dept. of Health and Human Services, 2012).

HIPAA does permit friends or family to pick up a prescription for a patient, but the pharmacist must use professional judgement in sharing PHI with the relative or friend. It is best to avoid discussion and encourage the patient to call with concerns. Similarly, a nurse should not disclose PHI with family members without the explicit consent of the patient.

Sign-in Sheets and Calls to Home

The HIPAA Privacy Rule also permits leaving a message on a machine or with someone who answers the phone when the patient is not home. Again, this is allowed as long as you:

- Reasonably safeguard the individual's privacy.
- Limit the amount of information you provide.

For example, if you are calling to follow up on a patient who has been discharged or to discuss a new prescription, you might want to consider leaving only your name and number and ask the individual to call back.

Requests for Access to Records

HIPAA outlines the requirements for sharing and reviewing medical records. Release of medical records can occur if the patient completes a HIPAA-compliant authorization form.

There are guidelines for when authorization is required and is not required. Authorization is not required when information is related for patient treatment issues. Authorization would be required to share PHI for life insurance review or to send lab reports to another entity.

The authorization includes the specifics of the PHI to be shared, the persons disclosing and receiving the information, expiration date and the right to revoke.

HIPAA also allows for the transfer of medical records in the event of a change of ownership of an organization. If you work in a pharmacy that acquires new ownership, the patient records are automatically transferred to the new owner. If the management of your organization changes at any time, the new management team has full legal access to all medical records maintained in that organization.

***Test Yourself*: A patient may request changes to their patient record and the covered entity must respond to the request within 30 days or request an extension of another 30 days with a valid reason. - True**

Each organization must determine the specific policies to be followed for that institution, but the following will be routine:

- Clear identification that the person requesting the medical record is either the patient or has the correct authorization to view the record.
- Only the parts of the record included in the authorization can be viewed.

- The patient may request changes to the record and the facility and parties involved must respond to the request within a preset time frame. Note that this does not imply that the record must be changed, only that the patient's request has a response.

Clear guidelines exist as to which staff members may have access to records and for what reasons.

***Did you know*? The final omnibus rule, passed in January 2013, clarifies the fact that genetic information is protected under the HIPAA Privacy Rule, and prohibits most health plans from using or disclosing genetic information for underwriting purposes.**

Emails Regarding Patients

Each organization will have specific guidelines but you are likely to see some or all of the following included:

- Do not put the patient's name or ID in the "subject line."
- Be certain you have the correct email address (watch for varying endings like .net, .com, .att, .edu, etc.).
- Only send necessary information in the email.
- Your facility may have a standard disclaimer at the end of each email sent.

All emails must be "encrypted," in other words, coded as they are transmitted and then "uncoded" at the receiving end.

Encryption is fairly standard for email transmissions in healthcare settings.

Faxes

HIPAA also covers fax communications with specific patient information. Although each organization will have different specific policies, general guidelines will most likely include the following:

- Locating fax machines in private and secure areas, away from patients and the public.
- Fax cover sheets will include a disclaimer to indicate what to do if sent inadvertently to the wrong number.
- Whether faxes can or cannot be sent during "off hours" when the receiving fax papers will not be picked up immediately.
- Protection of "Sent" faxes left unattended on the fax machine.

Computers

Computers allow access to a vast amount of patient information that must be secured.

Be vigilant about your computer use, following these guidelines:

- Computers should be set up so that the screens are not easily visible to the public or the patient.
- The computer user should "log off" when finished with the computer, so the screen is not left "on" and "visible" to others.
- Each computer user should have their own password so that each person using the computer and the screens they go to can be identified.
- Do not share your password with others.

Guidelines for Releasing Information

If the patient elects to be listed in a facility patient directory, the information in the directory may be released

to family, friends or the press. Similarly, under HIPAA law, a pharmacist may provide advice to customers regarding over-the-counter medications without signed consent.

Under HIPAA law, patients have the right to request a list of any instances, going back a period of 6 years or less, in which their information was disclosed to anybody outside the realm of treatment, payment or regular operations. This requires the maintenance of confidential record keeping for a minimum period of 6 years.

Once requested by a patient, the healthcare professional will have 60 days in which to provide the patient with an accounting of these disclosures, including the date, name and address of the person to whom the information was given, a brief description of the disclosure and the reason for it. This is for non-routine uses only. However, a healthcare professional does not have to account for disclosures that concern treatment, billing or accounting or for any disclosures made pursuant to receiving patient authorization.

Patients have a right to receive a copy of their medical and pharmacy records within 30 days of receipt of a written request. This time period may be extended an additional 30 days if a valid reason is given for the delay.

When No Information is Released

In general, any patient receiving care for substance abuse, psychiatric disorder, HIV, pregnancy, sexual abuse or rape is treated with an even greater level of confidentiality. Confirmation of the patient's treatment is generally prohibited. This means that if a call is received asking about a particular patient, no comment should be made as to whether the patient is even seeking treatment or being treated. Check with your organization's HIPAA policy for exact terminology.

Additionally, a patient may request to NOT be in the patient directory and the same standard would be in place. This is a critical feature and each organization will have very specific standards for you to follow.

***Test Yourself*: A patient must be listed on the patient directory so that their healthcare provider will know where to find them. – False, a patient can request not to be listed on the patient directory.**

Rights of Minors

The privacy rights of a minor have always been confusing for healthcare professionals. HIPAA does not specifically address the privacy issues of minors but directs the healthcare professional to follow the guidelines of the state law. This requires you to become familiar with the law in your particular state.

Each state varies on the age of majority (full adult rights and responsibilities) and on parental notification regarding medical treatment, birth control and other sensitive issues. It is thus advisable for the healthcare professional to formulate an ethical, standardized approach to these situations that all members of the organization adhere to, prior to the situation arising.

Unfortunately, many states do not stipulate exact standards for divulgence of minors' confidential information; and thus it is left to the discretion of the healthcare provider to use professional judgement.

An example of this would be a minor requesting birth control pills or treatment for a sexually transmittable disease. The healthcare professional should be familiar with the state law for the state in which he practices; but if the law does not specifically allow or disallow release of information to parents of a minor, then the healthcare professional will need to use their own professional judgement.

Always remember that HIPAA does not override state privacy laws. The healthcare professional must be familiar with the privacy laws in the state in which they practice.

Clergy

The HIPAA Privacy Rule allows clergy to be informed of parishioners that are in the hospital as long as the patient has been informed of this use and disclosure and does not object. This usually is included in the initial Privacy Notice that the patient receives on entering the hospital.

When, due to emergency circumstances or incapacity, the patient has not been provided an opportunity to agree or object, these disclosures may still occur. The disclosure must be consistent with any known prior expressed preference of the individual and the disclosure must be in the individual's best interest as determined in the professional judgment of the provider (US Dept. of Health and Human Services, 2012).

Authorized Disclosures

The HIPAA Privacy Rule does not require covered entities to obtain a patient's consent prior to using or disclosing protected health information about him or her for treatment, payment or healthcare operations.

This enables a pharmacist to use protected health information to fill a prescription that was telephoned in by a patient's physician without the patient's written consent, if the patient is new to the pharmacy.

Likewise, it allows a nurse to share protected health information about the patient with a dietician, occupational therapist or other allied healthcare worker who may need to be involved in the care of the patient.

The disclosure of the information, however, is always on a 'need to know basis.' A baby photographer on the postpartum floor may need access to the patient's name, room number and date of delivery of the infant in order to perform her duties, but does not need access to any other medical information.

Unauthorized Disclosures

Ensuring the security of patient information relies on your diligence. Unauthorized disclosures of protected information can occur if:

- You fail to ensure information you are sending is going to someone who is authorized to receive that information
- You neglect to review a patient's record to find restriction on the use of their information
- You hear discussions occurring in non-secure locations that disclose patient information

If you are aware of an incident that may have resulted in an unauthorized disclosure, you should report it immediately. Your facility may have a method to report unauthorized disclosures in a confidential manner.

***Test Yourself*: Unauthorized disclosures of protected information can occur if you fail to ensure information you are sending is going to someone who is authorized to receive that information. – True**

Penalties Under HIPAA

HIPAA authorizes the Secretary of Health and Human Services to impose civil as well as criminal penalties to covered entities, including pharmacies and hospitals, if they have violated the new privacy laws.

Fines can be as low as $100 for an inappropriate disclosure of a patient's PHI, up to $250,000 and ten years imprisonment for using PHI for commercial gain. This highlights the importance of protecting medical information from inappropriate usage.

Provided that all healthcare professionals follow the recommendations outlined in HIPAA, and take reasonable steps to protect the confidentiality of medical records, no criminal or civil suits will be instigated.

HIPAA requires each covered entity to appoint a Chief Privacy Officer, who is responsible for developing and implementing policies to comply with privacy rules; and a designated Contact Person to whom client complaints may be addressed. This may be the same person.

Chain pharmacies and affiliated hospitals that are under common ownership only need one privacy officer and contact person for the whole group.

HITECH Act of 2009

The Health Information Technology for Economic and Clinical Health Act (HITECH Act) is part of the American Recovery and Reinvestment Act of 2009 (ARRA).

ARRA contains incentives related to health care information technology in general, and contains specific incentives designed to accelerate the adoption of electronic health record (EHR) systems among providers.

In anticipation of a massive expansion in the exchange of electronic protected health information (ePHI), the HITECH Act widens the scope of privacy and security protections available under HIPAA; and increases the potential legal liability for non-compliance; and provides for more enforcement.

In 2011, the U.S. Department of Health and Human Services' (HHS) Office for Civil Rights (OCR) proposed changes to the Privacy Rule, pursuant to HITECH Act. It is proposed that individuals will be able to request an access report, which documents the particular persons who electronically accessed and viewed the individual's protected health information. At this time, covered entities are required to track access to electronic protected health information, but they are not currently required to share this information with the patient (HIPAA Survival Guide, 2012).

This proposed rule will require an accounting of more detailed information for certain disclosures that are most likely to affect a person's rights or interests. At the time of this course update, these changes have not yet been implemented to the Privacy Rule.

The Patient Protection & Affordable Care Act of 2010

The Patient Protection and Affordable Care Act was passed in 2010, and Provisions under the Affordable Care Act of 2010 will further these increases and include requirements to adopt:

- Operating rules for each of the HIPAA covered transactions
- A unique, standard Health Plan Identifier (HPID)
- A standard and operating rules for electronic funds transfer (EFT) and electronic remittance advice (RA) and claims attachments.

In addition, health plans will be required to certify their compliance. The Act provides for substantial penalties for failures to certify or comply with the new standards and operating rules.

The Final Rule

In January 2009, an addendum to HIPAA was added. This addendum facilitated the voluntary reporting of confidential patient information by all healthcare professionals to an independent organization, known as Patient Safety Organization (PSO).

This allows healthcare professionals to share with the PSO, any patient information relating to patient safety or quality of care concerns, without fear of liability. This will enable the PSO to analyze confidential patient safety events and make recommendations to improve the quality of patient care and improve safety standards.

In addition, certain provisions of HIPAA can be waived in certain circumstances during a national or public health emergency.

In January 2013, further privacy and security protections were added to the HIPAA law to strengthen the ability of the US Department of Health & Human Services (USDHHS) to vigorously enforce the HIPAA privacy and security protections.

Additional information can be accessed at the HIPAA website at: http://www.hhs.gov/ocr/privacy.

Conclusion

As this course has illustrated, HIPAA guidelines are in place to protect your patient.

Remember that each organization has the discretion to design policies and procedures within its system that meet the HIPAA guidelines but also provide a "fit" for the organization.

Although you may see variations in policies at different organizations, you will recognize that the overall intent is to improve the protection of patient confidentiality in a healthcare environment that includes a great deal of technological advances.

Review the specifics of your organization's policies and procedures to be certain that you know how to protect confidential medical information.

For additional HIPAA information, please visit the Centers for Medicare and Medicaid Services website at: http://www.cms.hhs.gov/hipaaGenInfo/

References

Centers for Medicaid & Medicare Services (CMS) (2012). HIPAA - General Information. Updated August 23, 2012 from: http://www.cms.gov/Regulations-and-Guidance/HIPAA-Administrative-Simplification/HIPAAGenInfo/index.html?redirect=/hipaaGenInfo/

HIPAA Survival Guide (2012). HITECH Act Summary. Retrieved August 28, 2012 from: http://www.hipaasurvivalguide.com/hitech-act-summary.php

US Department of Health & Human Services (2011). HHS announces proposed changes to HIPAA Privacy Rule. Retrieved August 27, 2012 from: http://www.hhs.gov/news/press/2011pres/05/20110531c.html

U.S. Department of Health and Human Services (2012). Where can I find information about HIPAA, health information privacy or security rules? Guidance Materials for Consumer. Updated August 22, 2012 from

http://answers.hhs.gov/questions/6180

U.S. Department of Health and Human Services Office for Civil Rights (2012). A Health Care Provider's Guide to the HIPAA Privacy Rule: Communicating with a Patient's Family, Friends, or Others Involved in the Patient's Care. Retrieved August 28, 2012 from: http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/provider_ffg.pdf

At the time this course was constructed all URL's in the reference list were current and accessible. rn.com is committed to providing healthcare professionals with the most up to date information available.

Disclaimer

This publication is intended solely for the educational use of healthcare professionals taking this course, for credit, from RN.com, in accordance with RN.com terms of use. It is designed to assist healthcare professionals, including nurses, in addressing many issues associated with healthcare. The guidance provided in this publication is general in nature, and is not designed to address any specific situation. As always, in assessing and responding to specific patient care situations, healthcare professionals must use their judgment, as well as follow the policies of their organization and any applicable law. This publication in no way absolves facilities of their responsibility for the appropriate orientation of healthcare professionals. Healthcare organizations using this publication as a part of their own orientation processes should review the contents of this publication to ensure accuracy and compliance before using this publication. Healthcare providers, hospitals and facilities that use this publication agree to defend and indemnify, and shall hold RN.com, including its parent(s), subsidiaries, affiliates, officers/directors, and employees from liability resulting from the use of this publication. The contents of this publication may not be reproduced without written permission from RN.com.

Participants are advised that the accredited status of RN.com does not imply endorsement by the provider or ANCC of any products/therapeutics mentioned in this course. The information in the course is for educational purposes only. There is no "off label" usage of drugs or products discussed in this course.

You may find that both generic and trade names are used in courses produced by RN.com. The use of trade names does not indicate any preference of one trade named agent or company over another. Trade names are provided to enhance recognition of agents described in the course.

Note: All dosages given are for adults unless otherwise stated. The information on medications contained in this course is not meant to be prescriptive or all-encompassing. You are encouraged to consult with physicians and pharmacists about all medication issues for your patients.

Please Read:

This publication is intended solely for the use of healthcare professionals taking this course, for credit, from RN.com. It is designed to assist healthcare professionals, including nurses, in addressing many issues associated with healthcare. The guidance provided in this publication is general in nature, and is not designed to address any specific situation. This publication in no way absolves facilities of their responsibility for the appropriate orientation of healthcare professionals. Hospitals or other organizations using this publication as a part of their own orientation processes should review the contents of this publication to ensure accuracy and compliance before using this publication. Hospitals and facilities that use this publication agree to defend and indemnify, and shall hold RN.com, including its parent(s), subsidiaries, affiliates, officers/directors and employees from liability resulting from the use of this publication. The contents of this publication may not be reproduced without written permission from RN.com.