HIPAA RULES AND REGULATIONS

INTRODUCTION

Everyone who works in health care is aware of the Health Insurance Portability and Accountability Act, which is commonly abbreviated as HIPAA. And everyone who is in the health care field has received printed material about HIPAA, has attended lectures about HIPAA, or attended mandatory education sessions that are designed to help staff understand how HIPAA affects the way they do their job and how to be HIPAA-compliant.

However, even though the federal legislation that enacted HIPAA was passed in 1996, many health care professionals are still unsure about exactly what HIPAA is, what it requires, and how HIPAA rules and regulations affect their practice on a day-to-day basis.

When you are working as a Certified Nursing Assistant (CNA), you will be responsible for understanding and using some parts of HIPAA. HIPAA may initially seem complicated, but the practical applications of HIPAA are not really that difficult and once you understand the three components of HIPAA, which are privacy, security, and administrative simplification - and particularly the first two - then HIPAA and the role it plays in your working day becomes clear.

STATEMENT OF PURPOSE

This module is intended to provide CNAs with information about HIPAA and to inform CNAs about what they need to know and do to be HIPAA-complaint.

THE HISTORY AND FORMATION OF HIPAA

The HIPAA legislation was enacted in 1996 and the original HIPAA legislation had two sections. The first part was concerned with making sure that health care coverage was available to workers and their families when an employee changed or lost his/her job.

The other part of the HIPAA legislation, the section that concerns and affects health care professionals, was generated in response to the growing use of electronic records and the increasing size and complexity of the health care system. It was becoming clear that with the change in the way information was generated, transmitted, and stored in hospitals, health care facilities, physician's offices, etc., that there was a significant potential for loss of privacy, and for misuse, abuse, and theft of patient information. It was also obvious that it was time for national standards that clearly outlined how confidential medical information should be handled. So, in response to those concerns the HIPAA legislation was created and put into place. Although there are many parts to HIPPA, the primary goal of HIPAA is to protect a patient's privacy.

When you first read about HIPAA or attend a HIPAA training class the topic is complex and confusing, and the idea of using HIPAA in the workplace can seem intimidating. But HIPAA can be easily understood by breaking it down into its

three main components and using HIPAA in the workplace is not complicated. The final section of this module will present examples of typical situations in which questions about the proper use of HIPAA might arise.

THE THREE COMPONENTS OF HIPAA

It was mentioned in the introduction that there are three components of HIPAA: privacy, security, and administrative simplification. Although each of these will be discussed separately, you will see as you read through the module that they are interdependent and are designed to be used together to protect patient privacy. The following points illustrate how the three components of HIPAA work as a whole.

- Health information is protected and the sharing and transmission of health information is controlled and regulated.
- Patients are notified of their privacy rights.
- Covered entities and their employees and healthcare professionals are required to adhere to HIPAA rules and regulations. A covered entity is any organization that routinely handles protected health information.
- Covered entities are required to educate their employees about HIPAA and to monitor themselves and their employees regarding adherence to HIPAA rules and regulations.
- Covered entities are required to make sure that protected health information is secure and is shared and transmitted safely and appropriately.
- Any breach in the securing or transmission of protected health information must be addressed by the covered entity. The covered entity must notify individuals whose protected health information has been compromised; they may be required to notify the media, and they must notify the U.S. Department of Health and Human Services (DHHS).

PRIVACY

Privacy is the most important part of HIPAA. Although there are HIPAA rules and regulations about security of information and safe transmission of information, those parts of HIPAA have their foundation in a concern for patient privacy.

Privacy is the easiest aspect of HIPAA to understand because the concept of privacy is universal; it is something everyone understands. We all consider parts of life to be private, and it is felt to be improper to ask someone about certain

topics such as her/his political opinions or religious beliefs. Private information is controlled - or should be controlled - by the person to whom it pertains.

The privacy section of HIPAA is the rules and regulations that specify how and when health care facilities, health care professionals, employers, and health insurance companies protected health information. Understanding the concept of protected health information is essential for being compliant with HIPAA and the following points should be read carefully.

Table 1: Key Points of the HIPAA Privacy Rules and Regulations

1. Protected health information is identifiable patient information that also contains:
   a. Any information that concerns the health status of an individual.
   b) Information about medical or psychiatric care that has been delivered, is being delivered, or will be delivered; care that has been delivered.
   c) Any information about genetic tests; genetic information about the patient or the patient's family; a request for genetic services or testing; participation in medical research that involves genetic diseases or genetic services, either for a patient or a patient's family member.
   d. Information about the financial aspects of or payment for medical or psychiatric treatment.
   e) Any information about the financial aspect of, or payment for that medical coverage.

   Note that the HIPAA rules and regulations state that protected health information is identifiable. That means that information about patient care must be accompanied by something such as a name, Social Security number, or address that can be used to identify the patient and associate him/her with medical or psychiatric care that is, has been, or will be delivered.

2. Protected health information can be electronic, verbal, or written.

3. The patient makes the final decision as to whom and how her/his protected health information can be shared and must be notified prior to sharing or transmitting protected health information. Prior notification is not required in certain circumstances; these will be discussed later in the module.

4. Protected health information can only be shared with or transmitted to someone or a specific entity (eg, a physician, an insurance company) that has a legitimate and reasonable need for the information. A legitimate and reasonable need for protected health information would include:
   a. Providing care to a patient.
   b. Ensuring patient safety.
   c. Providing information to someone who has and will be providing care for a patient.

d. Helping to facilitate the delivery of or payment for patient care.

5. Protected health information may be shared with or transmitted to spouses, family members or friends if it is reasonable to assume that the patient would not object and this sharing is in the patient's best interests.

7. Protected health information must be shared or transmitted in a way that is safe, secure, and confidential; this is the responsibility of covered entities and healthcare professionals.

8. Covered entities and healthcare professionals must make a reasonable effort to identify someone with whom they are sharing protected health information. Note that the word reasonable is used and that this implies someone using her/his professional judgment about what is reasonable.

This seems at first glance to be a lot of information about a relatively simple concept. However, although the application of the HIPAA privacy rules and regulations can at times be challenging the essence of these rules and regulations are simple.

Protected health information can only be shared with those who have a legitimate need to know, it must be shared in a way that protects patient privacy, and the patient is the final arbiter of what can be shared and with whom.

The Patient and HIPAA: Notice of Privacy Practice

The patient must be informed that her/his protected health information will be shared and transmitted. However, it is not necessary nor is it practical that this be done each time sharing or transmitting occurs. HIPAA simply requires that patients be given prior notice that this information will or might be shared and transmitted, and the prior notice is in the form of a notice of privacy practice. You do not have to familiarize yourself with every part of the notice of privacy practice form, but understanding its basics if helpful if you need to explain it to a patient.

The notice of privacy practice form is typically given to a patient during her/his first visit to a covered entity. The patient is asked to sign the notice and is given a copy, and the HIPAA rules in this regard state that "a covered health care provider with a direct treatment relationship with individuals must make a good faith effort to obtain written acknowledgments from those individuals that they have received the provider's notice . . ." The notice of privacy practice might differ from place to place but it should contain the following.

Table 2: Notice Of Privacy Practice

1. An explanation (and perhaps several examples) of situations in which protected health information is shared. For example, the protected health information may be shared if doing so will help assess, diagnose, or treat a

patient. This part of the notice of privacy practice essentially allows the health care provider to share protected health information if this sharing is felt to be in the best interest of the patient.

2. A description of who protected health information may be shared with, including insurance companies and third party payers and family members and friends.

3. Permission for the covered entity and health care professionals from whom you have received care to contact you and leave messages regarding your health.

4. An explanation of patient rights under HIPAA, eg, the patient can request that the covered entity disclose who his/her protected health information has been disclosed to.

5. An explanation of the responsibilities of the covered entity regarding the use, safety, security, and transmission of protected health information.

The notice of privacy practice can be bit confusing and especially so for patients, as they are given a notice of privacy practice each time they use the services of a covered entity. This may seem redundant and patients may wonder why it is done, but these notices are in a sense an agreement, a contract between the patient and the specific physician, hospital, etc. The purpose of the notice is to inform the patient that the covered entity is HIPAA-compliant; that the patient's protected health information will be used appropriately and safely; to explain to the patient how and why her/his protected health information will be used, and; to inform the patient of his/her HIPAA rights.

It was mentioned previously that there are circumstances in which prior notification of sharing/transmitting protected health information is not required. These circumstances include, but are not limited to: 1) Care delivered during an emergency; 2) Situations in which there are communication/language barriers but it is reasonable to assume that the patient would want care delivered and protected health information shared/transmitted; 3) If another covered entity or healthcare provided has asked that care be delivered, and; 4) Situations in which health care services are being provided to an inmate.

The HIPAA requirements for privacy are not suspended during an emergency but it is recognized that at times these requirements may be relaxed to protect public health and prevent disasters. The U.S. DHHS, which is the government agency involved in HIPAA, notes on its website that:

"Health care providers may share patient information with anyone as necessary to prevent or lessen a serious and imminent threat to the health and safety of a person or the public – consistent with applicable law (such as state statutes, regulations, or case law) and the provider's standards of ethical conduct. See 45 CFR 164.512(j)."

Summary

The privacy section of HIPAA can seem complex and confusing, and it does contain a lot of information. However, when working with HIPAA on the job, being compliant with HIPAA privacy rules and regulations is often a matter of judgment and common sense and the privacy aspect of HIPAA can be summarized as follows.

As a healthcare professional you must make sure that a patient's protected health information is only shared with the appropriate people in an appropriate way. If you keep in mind that sharing of protected health information can only be done for the purposes of providing treatment to a patient, ensuring patient safety, or facilitating payment for medical care, it is then obvious who can be told what about whom and when, where, and how this information can be shared. In addition, a patient's protected health information should only be shared if he/she has expressed permission that it is permissible to do so - if the patient has received and signed a privacy notice of privacy practice. If that seems too complicated then whenever you are unsure about HIPAA privacy rules and regulations ask yourself these questions. These questions could be considered to be a “formula: that you can apply if and when you are unsure how HIPAA applies to a particular situation.

1) Is the information that is being requested or may be shared protected health information?
2) Does someone have a legitimate and reasonable need to know protected health information about a patient?
3) Do you know the person who is asking for the information or if you don’t, have you made a reasonable attempt to identify them?

The US DHSS website has a very extensive section about HIPAA that can help answer your questions about HIPAA privacy rules or regulations (Or any other HIPAA topic). The website address is provided below and once you are on the site there is a list of HIPAA topics and also the option to ask a specific question about HIPAA.

http://www.hhs.gov/ocr/privacy/hipaa/faq/index.html.

SECURITY

The security section of HIPAA and the privacy section are closely related, but the privacy section outlines in general terms how to handle patients' protected health information that is written or electronic form. The security section is concerned with electronic protected heath information, and it outlines specific security safeguards that must be used by covered entities in order to keep protected health information safe and make sure it is used appropriately. In short, the privacy section of HIPAA tells you what to do: the security section tells you how to do it. The U.S. DDHHS website notes that:

"The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information."

The covered entity is required to put into place the security safeguards, monitor their effectiveness, and make sure that employees use them. The HIPAA required security safeguards include the following.

Administrative safeguards: Administrative safeguards are the policies and procedures that covered entities must put in place to safeguard protected health information. For example, this part of the security aspect of HIPAA dictates that covered entities must have a HIPAA privacy officer, they must have an emergency plan in case the security of the protected health information is compromised, they must clearly identify which employees are allowed to access protected health information, etc. In order to be HIPPA-compliant a covered entity must have written documented plans that address how it handles information security.

Physical safeguards: Physical safeguards are measures that are used to physically control access to protected health information. Examples: The electronic health information and the computer system that stores and transmits it must be closely monitored, access privileges to the computer clearly outlined and closely monitored, and workstation security must be ensured. These aspects of HIPAA security can be very important to CNAs and will be discussed in more detail.

Technical safeguards: The technical safeguards are, in large part, the responsibility of the computer professionals of each covered entity. HIPAA requires that the computer system of each covered entity be safe and secure from intrusion, have appropriate back-up systems, have procedures in place for safe information storage, retrieval, and transmission, and that any changes in the system that affect security be documented. This part of the security aspect of HIPAA is not typically something that concerns someone involved in direct patient. However, health care professionals do need to be aware that electronic information systems can be compromised and can break down. These problems can affect patient privacy, so if you notice something wrong with the system you are working with notify the appropriate person immediately.

HIPAA Security and the Workplace

You are familiar with the privacy requirements of HIPAA and you know that protected health information must be secured and protected, but in a busy workplace you need to know how to do so. According to the U.S. Department of Health and Human Services: "The Privacy Rule allows covered health care

providers to share protected health information for treatment purposes without patient authorization, as long as they use reasonable safeguards when doing so."

As with so much of HIPAA, the security requirements are specific but they essentially only ask for a reasonable level of care: HIPAA does not ask that healthcare professionals go to extraordinary lengths to safeguard protected health information. Remembering that protected health information can be electronic, verbal, or written and you will be HIPAA-compliant if you observe these following guidelines.

Electronic: "The Security Rule does not expressly prohibit the use of email for sending e-PHI (electronic protected health information). However, the standards for access control (45 CFR § 164.312(a)), integrity (45 CFR § 164.312(c)(1)), and transmission security (45 CFR § 164.312(e)(1)) require covered entities to implement policies and procedures to restrict access to, protect the integrity of, and guard against unauthorized access to e-PHI." If you are sending protected health information you must confirm the email address of the entity or person to whom you are sending the e-PHI to, and you should confirm that that the email was received: simple and reasonable. Texting protected health information is acceptable.

Verbal: Never discuss protected health information in a place or situation where it can be overheard by someone who does not have a legitimate need to know, and never discuss protected health information if there is no express or implied consent by the patient that the information can be shared. Given the environment of health care facilities this may seem to be impossible at times. For example, emergency rooms, clinics and other health care facilities often do not have a physical layout that provides complete privacy, and family members and friends or strangers may be present when protected health information is discussed. These situations will be discussed in a later section of the module. When you are discussing protected health information by telephone, do so discretely and always verify the identity and telephone number of the entity or person to whom you are speaking. Remember, it is only required that you make a reasonable effort to verify someone's identity.

Written: It is required that the transmission of written protected health information, by mail or fax, be safe and secure and that reasonable efforts are made to ensure this. If sending something by mail confirm the mailing address and make arrangements for a follow-up to be sure the item was received. If you are faxing, do not include protected health information on the cover sheet. Confirm the fax number and the name of the recipient before you send a fax and make arrangements for a follow-up to ensure the fax was received. These recommendations are supported by the US DHHS website. "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."

If you are not sure how to be HIPAA-compliant there are several options. Many health care facilities have a manual that explains HIPAA policy and how to apply it. There should also be someone in the facility who is designated to be a resource person for questions about HIPAA. And finally, the DHHS website is very user friendly and many questions about HIPAA and how to be HIPAA-compliant can be quickly and simply answered by using it.

HIPAA and Computer Security

As with all aspects of HIPAA compliance, following the HIPAA rules and regulations as they apply to computer security only requires you to use simple and reasonable precautions.

1. Never share your password with anyone, and always make your password is secure.

2. Make every practical and reasonable effort to ensure that computer screens that are showing protected health information are not visible to anyone who does not have a legitimate need to see the information.

3. Always log off after you have finished at a computer workstation.

Summary

The HIPAA security rule and regulations tells us in practical terms how to safely share and transmit electronic, verbal and written forms of protected health information and how to make sure this information is secure. These rules and regulations, as with many parts of HIPAA, require you to use simple and reasonable precautions and these precautions can be easily summarized.

First, make a reasonable effort to verify the identification of the person or entity with whom you will be sharing the protected health information.

Second, verify the correct email address, mailing address, telephone number of the recipient.

Third, verify that the information has been received.

ADMINISTRATIVE SIMPLIFICATION

The administrative simplification section of HIPAA involves a national standard for electronically transmitting information and a series of standard codes that covered entities must use to identify diagnoses, diseases, injuries, and other medical conditions. It also established a uniform system of electronic information exchange about the financial aspects of patient care. Administrative simplification is intended to streamline and standardize the administrative and financial aspects of providing care.

Certified nursing assistants are direct care providers. The administrative simplification section of HIPAA will not, for the most part, affect how CNAs work. The only possible effect administrative simplification would have for direct care providers would changes in forms, data gathering processes, etc.

USING HIPAA IN THE WORKPLACE

Understanding the different parts of HIPAA is important and it is the first step to using HIPAA. But the obvious question that everyone has is how does HIPAA change the way I work? What sorts of activities does HIPAA allow and what does it prohibit? Am I obeying or disobeying HIPAA regulations if I discuss a patient's condition with his/her family? Do HIPAA regulations mean that a patient cannot call his/her physician's office to obtain laboratory test results? Am I violating HIPAA regulations if I call a patient by name in front of other people in a busy waiting room? When you think about what HIPAA means, using it can begin to seem very complicated.

Fortunately, using HIPAA is not that difficult. All covered entities should have a HIPAA information manual you can refer to, and there should also be a staff member who is a HIPAA resource. So if you have a question about HIPAA, you can look up the answer or ask the HIPAA resource staff person.

More importantly, although there are many "do's and don'ts" of HIPAA, if you remember the following two statements, you will always understand what you should and should not do with protected health information.

- Protected health information is information that would reasonably be considered private.

- Protected health information should only be shared with appropriate people in an appropriate way and in an appropriate place.

Remember, HIPAA governs what you write and what you send through a computer, but HIPAA also governs what you say. Verbal transmission of protected health information is also covered by HIPAA.

The following scenarios provide examples of using HIPAA in the 'real world," and they are situations that you will most likely encounter.

Scenario #1: A patient informs you that he has tuberculosis, but he has not told his physician or anyone else. You decide not to tell anyone because the patient did not give you permission to do so and this is information that would reasonably be considered private and protected. Right or wrong?

Answer: Wrong. You are correct that this information is private and that protected health information should only be shared if the patient has given permission, and it should only be shared with the appropriate people. However, there are exceptions to this rule. If the patient has a gunshot, is a victim of abuse, or has certain communicable diseases, this information can be divulged to public

health agencies or appropriate care givers. These are considered reportable diseases or incidents, and the concern for public health and the law supersedes the patient's right to privacy. Tuberculosis is spread by inhalation of infected airborne droplets. However, wearing a mask or a respirator is not part of Standard Precautions and it is not possible to know at a glance if someone has active tuberculosis and is infectious. Therefore, healthcare personnel and the public have a legitimate need to know about this.

Scenario # 2: You are caring for a patient who is visiting a clinic for a minor injury. The patient tells you that she is infected with the hepatitis C virus, but that she has not divulged this information to anyone else. Because of the potential risk of transmission and the seriousness of hepatitis C you decide to inform the other CNAs, the nurses, and the physician of what you know. Right or wrong?

Answer: Wrong. All health care providers should use universal precautions and these will prevent transmission of hepatitis C so it is not necessary to know a patient's status in this regard. In this situation there is no legitimate need to know about the hepatitis C infection.

Scenario #3: You are working at workstation entering information into a patient's chart. The computer screen is facing away from the hall, but glare from a window reflects on the screen. This makes reading the screen difficult so you turn it around. Then, someone asks you to assist with moving a patient out of bed, so you leave your note unfinished to go help. Right or wrong?

Answer: Wrong. A computer screen should never be made visible to anyone not involved with patient care, and you should always "hide" a computer screen that has patient information on it if you must interrupt data entry. Other important rules for using computers that involve HIPAA: never share your password with anyone, and always log off when you are finished with the computer.

Scenario #4: You notice that fax containing laboratory results has been transmitted. You are going to place the fax in a file, but you must answer a call light so you set it down on the desk. When you return, you realize that the same laboratory results are in the electronic record, so you throw the fax in the trash. Right or wrong?

Answer: Wrong. If you don't have time to properly file the fax, place it face down where it won't be noticed. If the fax isn't needed, place it in a shredder.

Scenario #5: You are in an elevator with a co-worker. One of your patients was just diagnosed with cancer, and you are discussing the patient's condition, without using her name, so although there are other people are in the elevator, you feel secure. Right or wrong?

Answer: Wrong. Never discuss protected health information unless you are sure that only appropriate people can hear the conversation. Although there is no identifiable information being used in the conversation, a public elevator is not a secure place and there is no need to discuss this situation in that area. In addition, there may be some part of the patient's condition that is unique and this could be considered identifying information.

Scenario #6: A physician working in a busy emergency room tells a patient that he has pneumonia. The patient is very ill and weak and cannot be moved so she must be told then and there. The emergency room is very crowded and other patients can hear the conversation. Is this a HIPAA violation?

Answer: No. Remember, one the guiding principles of HIPAA is being reasonable. As regarding situations such as the one outlined in Scenario # 6, the HIPA regulations again stress the need for being reasonable and understanding circumstances. "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 that reflect their particular circumstances . . . 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 for quick, effective, and high quality health care. The Privacy Rule also recognizes that overheard communications in these settings may be unavoidable and allows for these incidental disclosures."

Scenario # 7: You are working in a cardiologist's office and one of your responsibilities is to escort patients from the waiting room to an examination area and then take the patient's vital signs. You walk into the waiting are and call a patient's name, and he responds. By doing so have you disclosed protected health information? After all, you have identified the patient by name and because of the location you have, in a sense, disclosed that he has a cardiac problem. Is this a HIPAA violation?

Answer: No. First, you did not identify the patient; the patient identified himself. Second, by the patient's voluntary presence at the cardiologist's office he has willingly allowed anyone else in the waiting room to assume that he has, or may have a cardiac problem, but there is certainly no identification of what the problem could be, what treatments are being given, etc. And finally, there really is no reasonable alternative.

Scenario # 8: You witness a nurse discussing a patient's cancer treatments and there are several other people - family members and friends of the patient - in the room. The patient is awake and mentally competent. A co-worker mentions to you later in the day that this was HIPAA violation. Is it?

Answer: No. The patient gave implied consent for the protected health information to be disclosed by not objecting to the presence of these family members and friends.

Scenario # 9: You answer the telephone at work and someone identifies herself as a relative of a patient you are caring for, and asks you for an update on the patient's condition. You don't recognize the caller's name but she seems reasonable and pleasant so you decide to tell her as it seems impolite to quiz her about who she is. Right or wrong?

Answer: Wrong. If you don't recognize someone who is asking for protected health information and you can't easily verify the person's identity (As is the case here) then you should not disclose it. This is a very common situation and it can easily be avoided and/or handled. Find out from the patient who she/he would like to be provided with updates. You could also place the caller on hold and quickly check with the patient or have her call back later.

Scenario #10: Someone stops you in the hall and asks a question about the medical condition of one the patients you are caring for. This is the first time you have cared for this patient, but you have seen this person visiting the patient several times a day in the past week, so you give him a quick summary of the patient's health. Right or wrong?

Answer: Wrong. This person is probably a relative or a friend, but he could be anyone; you don't know. The patient is the one who decides who can have access to his/her protected health information, so in this situation you would have to check with the patient first. Protected health information can be disclosed to someone if the patient has agreed, if the person receiving the information is involved in some way in the patient's care, and if the information is needed for that person to be involved in the patient's care. The simplest and most graceful way to handle this situation is to ask the person his name and then quickly go to the patient, confirm the friendship, and confirm that sharing protected health information is acceptable to the patient.

Scenario #11: Someone asks you by telephone about the condition of a patient. She identifies herself as the patient's spouse but you have never met this person. You quickly explain privacy concerns and then ask her what her husband's birthday is and the name of his physician. She answers these questions correctly so you give her an update. Right or wrong?

Answer: Right. You have made a reasonable effort to identify this person so sharing protected health information in this situation is acceptable.

Scenario # 12: You want to send a fax that contains protected health information. You confirm the recipient's fax number and send the fax but after a

few minutes there is a message on the machine that the fax was not transmitted. You re-send the fax. Right or wrong?

Answer: Wrong. In this situation you should call the recipient to see if the fax was transmitted and received and to re-confirm their fax number. You should also check the fax machine to make sure the original message was sent to the proper number.

SUMMARY

HIPAA is primarily concerned with maintaining the safety and security of protected health information. Protected health information is defined as identifiable patient information that also contains:

1. Any information that concerns the health status of an individual.
2. Information about medical or psychiatric care that has been delivered, is being delivered, or will be delivered; care that has been delivered.
3. Any information about genetic tests; genetic information about the patient or the patient's family; a request for genetic services or testing; participation in medical research that involves genetic diseases or genetic services, either for a patient or a patient's family member.
4. Information about the financial aspects of or payment for medical or psychiatric treatment.
5. Any information about the financial aspect of, or payment for that medical coverage.

Protected health information can only be shared or transmitted to someone who has a legitimate need to know and if that person or entity has been identified or a reasonable attempt at identifying them has been made. In addition, the sharing or transmitting of protected health information must be done is a way that is safe and secure, and healthcare professionals and covered entities are expected to make reasonable efforts to endure safe and secure information transmission. This applies to electronic, verbal, and written forms of information sharing.

All covered entities must adhere to HIPAA privacy and security regulations: a covered entity is defined as any person or organization involved in the care or treatment of a patient *or* responsible for the financial aspects of patient care. Patients must be informed of their HIPAA rights and be provided with a notice of privacy practice that explains these rights.

If you have any questions about HIPAA or how to be HIPAA-compliant, check with a resource or simply as yourself the following questions: using them will ensure you are HIPAA-complaint.

1) Is the information that is being requested or may be shared protected health information?

2) Does someone have a legitimate and reasonable need to know protected health information about a patient?
3) Do you know the person who is asking for the information or if you don't, have you made a reasonable attempt to identify them?
4) Are you sharing/transmitting the protected health information in a way that is safe and secure?