



# **HIPAA**

## **Health Insurance Portability & Accountability Act**

**Inservice**

**Instructions: Please read, complete and return post-test.**



**PROTOCOLL**  
**Health Insurance Portability & Accountability Act**  
**(HIPPA)**  
**Education Packet**

The attached education document covers general information regarding the new Federal HIPPA Privacy regulatory act, which became effective 4/12/2003. This packet is part of mandatory education for all Protocol employees.

Please review the materials and complete the attached quiz at the end of the packet. The quiz should be returned to your supervisor as soon as possible.

If you have any additional questions or concerns, please contact:

Darlene Melfi  
Vice-President of Healthcare Operations  
856-227-1900 or 215-592-7400  
[dmelfi@protocolstaffing.com](mailto:dmelfi@protocolstaffing.com)



**PROTOCOL**  
**Health Insurance Portability & Accountability Act**  
**(HIPPA)**  
**Education Packet**

In 1996, the United States Congress passed the Health Insurance Portability and Accountability Act (HIPPA). The original goals of the legislation were to:

- Improve efficiency and effectiveness of the health care system by standardizing the electronic exchange of administrative financial data.
- Help people obtain and maintain their health insurance benefits when they changed jobs.

There are multiple parts of the law focusing on different rules of compliance that have different compliance dates. This training module focuses on the Privacy Rule, which became effective on April 14, 2003.

For the first time, the Privacy Rule creates a national standard to protect individual's medical record and other personal information.

Covered entities (such as Protocol) must:

- Notify clients of their privacy rights and how information can be used.
- Adopt and implement privacy procedures.
- Train employees so that they understand the privacy procedures.
- Designate an individual responsible to ensure privacy procedures are adopted and followed.
- Secure client records containing Protected Health Information (PHI) so that patient information is not available to those who do not need access to it.

If existing state regulation is more stringent than the HIPAA regulations, the state regulations must be followed.

The purpose of HIPPA is to improve the overall effectiveness and efficiency of the healthcare industry.

## GLOSSARY OF TERMS

To assist you in understanding HIPPA, the following terms used in the HIPPA training are defined below:

**Business Associates:** A person or entity that performs a certain function(s) or activities that involves the use or disclosure of protected health information on behalf of or provides services to, a covered entity.

**Covered Entity:** A healthcare provider, health plan or health care clearing house that transmits any health information electronically in connections with certain transactions.

**Health Care Provider:** Any person or organization who furnishes, bills or is paid for health care in the normal course of business.

**HIPPA:** An acronym for Health Insurance Portability and Accountability Act, a bill passed by Congress in 1996 that mandates the adoption of standards for the exchange of electronic health information in an effort to encourage overall administrative simplification.

**Incidental Use or Disclosure:** A secondary use in disclosure that cannot reasonably be prevented is limited in nature, and that occurs as a result of another use or disclosure that is permitted by the Rule.

**Minimum Necessary:** Policies and procedures that limit how much protected health information is used, disclosed, and requested for certain purposes. These minimum necessary policies and procedures also reasonably must limit who within the entity has access to protected health information, and under what conditions, based on job responsibilities and nature of the business.

**Notice of Privacy Practice:** Health plans and covered health care providers are required to develop and distribute a notice that provides a clear explanation of the privacy practices and to be informed of their privacy rights with respect to their personal health information. The notice is intended to focus individuals on privacy issues and concerns and to prompt them to have discussions with their health plans and health care providers and exercise their rights.

**Entity:** An existing business, in this law it refers to an existing healthcare business.

**PHI:** Another name/abbreviation for **Protected Health Information**. PHI refers to individually identifiable information that is transmitted by electronic media, maintained as electronic media, or transmitted or maintained in any other form or medium. This includes both medical information (such as ICD-9-CM codes) and information that could be used to identify a patient (such as their home address). PHI includes all of the following:

- √ Name
- √ Birth date
- √ Medical Record Number
- √ Account Number
- √ Photographic Images
- √ Address
- √ Phone number, email address, fax number
- √ Health Plan Number
- √ Name of Employer
- √ Social Security Number

**Privacy Rule:** One of the HIPPA regulations (others include Security and Electronic Transactions) that focuses on the standards for the privacy of individually identifiable health information. Clients have new rights to understand and control how their health information is used. Accountability for release of PHI is crucial. Penalties are hefty!

**Treatment, Payment, and Healthcare Operations:** "Treatment" generally means the provision, coordination, or management of health care and related services among health care providers or by a health care provider with a third party, consultation between health care providers regarding a patient, or the referral of a patient from one health care provider to another. "Payment" encompassed the various activities of health care providers to obtain premiums, to fulfill their coverage responsibilities and provide benefits under the plan, and to obtain or provide reimbursement for the provision of health care. "Health care operations" are certain administrative, financial, legal and quality improvement activities of a covered entity that are necessary to run its business and to support the core functions of treatment and payment.

Lack of compliance can result in prison sentences and/or fines.

For knowingly obtaining or disclosing identifiable health information, the following penalties may apply:

VIOLATION	PENALTY
Knowingly obtaining or disclosing identifiable health information except on a "need to know" basis in support of Treatment, Payment or Healthcare Operations.	Up to \$50,000 fine and one (1) year imprisonment.
The violation above committed under false pretenses.	Up to \$100,000 fine and five (5) years imprisonment.
The violation above committed with intent to sell, transfer, or use for commercial advantage, personal gain or malicious harm.	Up to \$250,000 fine and ten (10) years imprisonment.



## Notice of Privacy Practices

Covered entities must develop and provide individuals with notice of their privacy practices; the notice should state how a covered entity may use and disclose PHI about the individual, as well as his or her rights and the covered entity's obligations with respect to that information. Covered entities must give notice not later than the first service delivery and make a good faith effort to obtain the individual's written acknowledgement of the notice.

Protocall has developed a Notice of Privacy Practice. This notice will be given to all clients and given to the patient at the time of admission.

The notice:

- Describes how Protocall may use and disclose PHI for treatment, payment and healthcare operations (this is permitted by the Privacy Rule).
- Describes how the client can file a complaint if they believe their rights have been violated.

Through the notice, the client has the following rights:

- To request a limitation on his or her PHI that can be disclosed to someone involved in the client's care or payment for client's care, such as a family member or friend.
- To inspect or copy their PHI.
- To amend what they believe is incorrect or incomplete information in their record.
- To receive communications from Protocall on a confidential basis by receiving the information at an alternative address.

Protocall must make a good faith effort to obtain the client's written acknowledgement of receipt of the notice.

In an emergency situation, it is permitted to treat the client without giving the client the Privacy Notice, if obtaining the notice interferes with the ability to provide necessary medical attention. The Rule states that the client receives the notice when "practical" in such a situation.

In addition, under state or other applicable law, an authorized person may act on behalf of the individual in making health care related decisions as the individual's "personal representative". The representative must be treated as the individual for purposes of the Privacy Rule, where applicable.

## Incidental Uses and Disclosures/Minimum Necessary

The Privacy Rule permits certain incidental uses and disclosures of PHI to occur when the covered entity has in place reasonable safeguards and minimum necessary policies and procedures to protect an individual's privacy.

An incidental use is defined as: 'a secondary use or disclosure that cannot reasonably be prevented is limited in nature and that occurs as a result of another use or disclosure that is permitted by the Privacy Rule'.

For example, a visitor overhearing a provider's confidential conversation with a client is NOT a violation, if the provider has made a reasonable effort to safeguard the conversation (e.g., speaking in low voices and conversing in an appropriate area). **A discussion about a client's condition including PHI in a public area such as a church, school, or parking lot IS a Violation of the Privacy Rule.**

The minimum standard requires covered entities to evaluate their practices and enhance safeguards as needed to limit unnecessary or inappropriate disclosure of PHI.

This section allows:

- Nurses or other health care professionals to discuss a client's condition over the phone with the client, provider, or family member. Please note – a client has the right to "opt out" and have their information released or not to be released to certain individuals. And this must be verified before discussing the client's condition. Also an effort must be made to verify the IDENTITY of the individual making the request.
- A physician to discuss a client's condition or treatment regimen in the client's home.
- Healthcare professionals to discuss a client's condition during training in an academic training or institution.

In many cases, the Privacy Rule builds upon safeguards already in place, such as individual computer passwords for staff to access PHI; or isolating/locking file cabinets or records rooms. This section, in particular, stresses *common sense* that calls for a method consistent with the best practices and guidelines, already used by many providers and plans today *to limit the unnecessary sharing of medical information*.

These are examples of NOT following the minimum necessary guidelines:

- Use of sign in sheets that contain medical information about the client (sign in sheets without medical information are permitted).

## Incidental Uses and Disclosures/Minimum Necessary (cont'd)

- Allowing full access to medical records information to employees (except where employees need full access to provide treatment to the client).
- Leaving the client chart in an unsupervised area **without** regard to protecting the chart.

The computer directory is permitted to contain the client's name, general condition (using phrases: under evaluation, good fair, serious, or critical), and address of the client. The agency can also disclose the religious affiliation of the client to clergy where appropriate.

A client has the right to ask that their information not be available on the computer directory, or that their information be kept confidential for certain individuals.

**NO information may be released about a client unless expressly consented to by the client or the client's legal representative where applicable.**

Other important information:

Paper documents that contain PHI CANNOT be thrown into the trash, where it could be picked up and read. There will be containers where this information can be place for shredding. These containers will be stored in a secure location and then disposed of in an appropriate manner (such as shredding). It is permissible to shred the information on site, and then dispose of the shredded material. **Protocall will have a secure trash can in each office to put trash in for shredding.**

## Faxing of PHI:

When you don't know the requester, you must make a reasonable effort to determine that the protected health information is being to an entity authorized to receive it as follows:

- Ask for the telephone number of the office where the fax machine resides.
- Call the office number, and ask the person who answers to verify that the fax number is correct, and that the office is that of the individual requesting the fax.
- If the numbers DO NO MATCH, please report this to your supervisor for further instructions. DO NOT send the fax if there is any doubt about the receiver's identity.
- If the numbers match, send the fax with the approved Protocall cover sheet that includes the confidentiality statement.
- If you know the requester and have previously validated the fax number, send the fax with the approved Protocall cover sheet that includes the confidentiality statement.



## Faxing of PHI: (cont'd)

For Computerized automated faxing systems, the Vice President of Operations must establish an annual schedule for verification of the fax numbers within the system and document completion of the verification. The document will then be stored at the Privacy Office. All existing automated faxing systems should be verified by sending a 'HIPAA fax test" fax to all numbers in the system and requesting the receiver call us to verify that the fax number is correct. Any faxes sent that are not responded to should be called manually to verify that the fax number is correct.

**No one may send individually identifiable health information outside of Protocol electronically via Internet e-mail or any other electronic data transmission (including file transport protocol).** If there are circumstances where you believe it is imperative for you to do so, please have your office contact the Privacy Officer for assistance in the proper protocol.

## Business Associates

Protocol may disclose PHI to a third party who acts as a business associate only to help the agency carry out its health care functions. A business associate is a person or entity that performs certain functions or activities that involve use of disclosure of protected health information on behalf of, or provide services to, a covered entity.

Business associates must sign a business associate agreement that assures they will safeguard the information, states the permitted uses and disclosures, and requires the company to report any non-permitted uses and disclosures to Protocol. The minimum necessary rule applies and only necessary information can be released to a business associate.

All business associate contracts signed or renewed (non-automatically) after October 15, 2002 must have a business associate agreement in effect by April 14, 2003. All other contracts need a BAA by April 14, 2004 or by their renewal date whichever occurs first.

A software vendor who needs access to the application software for support and maintenance purposes and is exposed to PHI while troubleshooting would need a BAA. A housekeeping service that has incidental exposure or a software vendor who does not access a system with PHI does not need a BAA.

## Uses and Disclosures for Treatment, Payment, and Health Care Operations

Protocol may without the individual's consent use or disclose PHI for its own treatment, payment, and health care operations. An authorization is needed to disclose data for other purposes, including disclosure of PHI to a third party specified by the individual.



## **Uses and Disclosures for Treatment, Payment, and Health Care Operations (cont'd)**

PHI can be de-identified, and used for other purpose (e.g. recruitment), however the data must be certified as de-identified by a statistician or must be stripped of certain identifiers including name, address, city, zip code, and social security numbers).

### **Marketing**

With limited exceptions, the Rule requires an individual's written authorization before a use or disclosure of his or her PHI can be made for marketing purposes.

### **Disclosures for Public Health Activities**

The Rule permits covered entities to disclose PHI without authorization for specified public health purposes.

### **Workers Compensation Laws**

The Rule permits disclosures of health information for worker's compensation purposes without authorization covered under state or other laws related to the workers compensation, or to obtain payment for health care provided to the worker; and with authorization from the individual.

### **Government Access**

Covered entities must cooperate with efforts by the Department of Health and Human Services Office for Civil Rights to investigate complaints or otherwise ensure compliance.

### **More Information**

For more detailed information can be found at the following websites:

- ***The NJHA website:***  
[www.njha.com/HIPAA\\_section](http://www.njha.com/HIPAA_section)
- ***The United States Department of Health and Human Services website:***  
[www.hhs.gov/ocr/HIPAA](http://www.hhs.gov/ocr/HIPAA)
- ***HIPA Advisory website:***  
[www.hipaadvisory.com](http://www.hipaadvisory.com)



## Health Insurance Portability and Accountability Act (HIPAA) Post-Test

Name \_\_\_\_\_ Date \_\_\_\_\_

1). If state law is more restrictive than federal HIPAA law, which of the following is true?

- A. State law must be followed because it is more restrictive.
- B. Federal law must be followed because the federal law is more important than the state law.
- C. The privacy law was a decision made by U.S. citizens.

2). Which of the following is not considered a client right under the HIPAA?

- A. That the client's PHI that can be told to someone involved in their care or payment of their care.
- B. To inspect or copy their PHI.
- C. Receive a discount on their bill if they sign the Privacy Notice informal consent.
- D. Receive communications from Protocol at a different address.

3). Which of the following things must a covered entity not do under the HIPAA regulations?

- A. Notify clients of their privacy right and how information can be used.
- B. Refuse to treat a client who does not sign the Notice of Privacy Practice.
- C. Protect client records containing health information so that they are not available to those who do not need them.
- D. Shred all paper that has any confidential data relating to a client.

**TRUE OR FALSE (please circle the answer)**

4. Knowingly giving client health information is a violation of the Rule and may result in prison sentences and/or hefty fines. **TRUE or FALSE**

5. If a client cannot be given a privacy notice in an emergency situation, we do not have to give them a copy at a later date. **TRUE or FALSE**

6. A normal discussion about a client's condition in a public area such as the parking lot or elevator is a violation of the Privacy Rule. **TRUE or FALSE**

7. Clinicians or office staff can discuss any healthcare information with anyone who calls inquiring about a client. **TRUE or FALSE**

8. The nursing care plan can be shown to anyone coming into the home. **TRUE or FALSE**

9. It is important to log off the computer every night. **TRUE or FALSE**

10. PHI can be sent to anyone outside the institution through Email or phone without seeking guidance from the Privacy Officer. **TRUE or FALSE**