

## TUTORIAL

### Health Insurance Portability & Accountability Act (HIPAA)

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

- Improve efficiency and effectiveness of the healthcare 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 the compliance that have different compliance dates.

This training module focuses on the Privacy rules, 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 *CareCo Continuum*) must:

- Notify clients of their privacy rights and how information can be used.
- Adopt and implement privacy procedures.
- Train employees so that they can understand the privacy
- 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 the existing state regulation is more stringent than the HIPAA regulations, the state regulation must be followed.

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

**Privacy Rule:** One of the HIPAA regulations (other includes 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 healthcare providers or by a



health care provider with a third party, consultation between health care providers regarding a patient, or the referrals 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 provides benefits under the plan, and to obtain or provides reimbursement for the provision of quality improvement activities of a covered entity that are necessary to run its business and to support the core functions of treatment and payments.

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 health information except on a "need to know" basis in support of Treatment, Payment or Healthcare Operations- Up to a \$50,000 fine and one (1) year of imprisonment.

The violation above committed under false pretenses- Up to a \$100,000 fine and five (5) years imprisonment.

The violation above committed with intent to sell, transfer, or use for commercial. Personal gain or malicious harm. – Up to a \$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 acknowledgment of the notice.

**CareCo Continuum**, 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.

This section **allows**:

- Nurses or other healthcare 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 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 a guideline 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).
- 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 placed 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. **CareCo Continuum** has a container for the PHI located in the main lobby.

#### **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 sent 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 NOT 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 **CareCo Continuum** 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 CareCo Continuum, Inc. cover sheet that includes the confidentiality statement.

**No one may send individually identifiable health information outside of *CareCo Continuum* electronically via Internet e-mail or any other electronic data transmission.**

## **BUSINESS ASSOCIATES**

**CareCo Continuum** 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 **CareCo Continuum**. The minimum necessary rule applies and only necessary information can be released to business associate.

## **GLOSSARY OF TERMS**

To assist you in understanding HIPAA, the following terms used in the HIPAA 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 healthcare clearinghouse that transmits any health information electronically connection with certain transactions.

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



**HIPAA:** 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 healthcare 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 healthcare 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 IC-10-CM codes) and information that could be used to identify a patient (such as their home address). PHS includes all of the following:

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

The Notice:

- Describes how **CareCo Continuum** 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 notice, the client has the follow rights:
- To request a limitation on his or her PHI that can be disclosed to someone involved in the clients 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 and incomplete information in their record.



- To receive communications from **CareCo Continuum** on a confidential basis by receiving the information at an alternative address.

**CareCo Continuum** must make a good faith effort to obtain the client’s written acknowledgment of receipt of the notes. 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 healthcare related decisions as the individual’s “personal representative.” The representative must be treated as the individual for purposes of the Privacy Rule, were applicable.

### **INCIDENTAL USES AND DISCLOSURE/MINIMUM NECESSARY**

The Privacy Rule permits certain incidental uses and disclosure 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 appropriate area). **A discussion about a client’s condition including PHI in a public area such as 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.

### **USES AND DISCLOSURES FOR**

#### **Treatment, Payment, and Healthcare Operations**

**CareCo Continuum, Inc.** may without the individual’s consent use or disclose PHI for its own treatment, payment, and healthcare operations. An authorization is needed to disclose data for other purposes, including disclosure of PHI to a third part specified by the individual. PHI can be de-identified, and used for other purposes (e.g. recruitment), however the date must be certified as de-identified by 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/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 disclosure of health information for worker's comp purposes without authorization covered under state or other laws related to the workers compensation, or to obtain payment for healthcare provided to the worker; and with authorization from the individual.

**Government Access**

Covered entities must cooperate with the 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 visit the following websites:

**-The NJHA website**

- [www.njha.com/HIPPA](http://www.njha.com/HIPPA)

**- The United States Department of Health and Human Services Website**

- [www.hhs.gov/ocr/HIPPA](http://www.hhs.gov/ocr/HIPPA)

**- HIPPA Advisory website**

- [www.hipaaadvisory.com](http://www.hipaaadvisory.com)