HIPAA Employee Training Guide

Revised November, 2017

What is HIPAA?

The Health Insurance Portability and Accountability Act of 1996 (also known as "Kennedy-Kassebaum Act").

HIPAA regulations address the use and disclosure of Protected Health Information (PHI).

Key HIPAA Elements:

- Health Insurance Portability
- Standards for Electronic Claims Submission
- Security and Privacy Protection

Security and Privacy are addressed in this Training Guide.

Who is covered by HIPAA?

Covered Entities (CEs) are organizations that are required to comply with HIPAA standards. There are three types of covered entities:

1. Health plans
2. Health care clearinghouses
3. **Health care providers*** who transmit any health information in electronic form in connection with one of the standard transactions.

***** Consumer Direct is a health care provider and therefore considered a CE.

When did the "HIPAA Privacy Rule" go into effect?

Effective as of April 14, 2003; Revised January 25, 2013

What is PHI (Protected Health Information)?

PHI is any health information that contains a unique identifier (to a patient) such as full name, social security number, phone number, etc. PHI is to be protected and kept confidential, whether in **handwritten, printed, electronic, or verbal form**.

Patients Will Be Notified of Their HIPAA Rights

Each patient will receive the Consumer Direct Notice of Privacy Practices which explains how medical information may be used and disclosed, and how the patient can access their information. **Ask a Program Manager or the Privacy Officer if you have or receive questions.**

Patients Can Request Confidential Communication

Consumer Direct will accommodate reasonable requests from patients to use alternate channels of communication (e.g. work telephone instead of home telephone, alternate mailing address, etc.). **Ask a Program Manager if you have questions.**

When is "Authorization to Release Information" NOT required by the Patient?

For treatment, payment, or healthcare operations.

What are HIPAA "Uses and Disclosures" of PHI?

Use: The sharing, employment, application, utilization, examination, or analysis of such information by an entity that maintains such information.
Disclosure: The release, transfer, provision or access to, or divulging in any other manner of information outside the entity holding the information.

Patients Access to Medical Records

Patients may wish to view information in their medical records and may express disagreement with its content. Consumer Direct has procedures in place for patients to request access and make corrections to their Consumer Direct records. In the event of any such request by a patient, **ask a Program Manager or the Privacy Officer for assistance.**

"TOP TEN" HIPAA Tasks

1. Assign overall responsibility for privacy and security.
   *The Consumer Direct **Privacy Officer is Daryl Holzer,** who has overall responsibility for privacy issues. **Program Managers** are available to address any HIPAA-related questions. **Jeff Harriott** is the **Security Official** responsible for security measures.*

2. Establish procedures for handling PHI.
   *Consumer Direct has a Privacy Policy (a copy of which is enclosed in this Training Guide) and a Privacy Manual with which to manage privacy issues. **A Program Manager or the Privacy Officer can address your questions.***

3. Provide physical security.
   Includes physical security of office facilities, medical records, billing information, and other PHI. Physical security measures may include using locking file cabinets where PHI is stored.

4. Provide technical security.
   Includes securing information stored and transmitted via computers.

5. Establish rules for protecting patient privacy.
   This is an essential part of maintaining patient confidentiality. Consumer Direct has Patient Confidentiality requirements outlined in the Employee Handbook that require each employee to maintain the confidentiality of patient information.

6. Allow patient access to medical records.
   *Patients have the ability to access their medical information and have control over who may review their information. **Ask a Program Manager for more information.***

7. Respond to complaints
   Consumer Direct has HIPAA compliant forms available for handling any complaint that may occur as a result of privacy protection. ***Ask a Program Manager for more information.***

8. Publish a Notice of Privacy Practices.
   Consumer Direct has posted a ***N****otice of* ***P****rivacy* ***P****ractices (NPP) and also provided written notice to each of our patients regarding their rights.*

9. Ensure that Business Associates protect patient privacy.
   Business Associates are not Covered Entities (health care providers), like outside consultants, who may come in contact with our Protected Health Information. Consumer Direct will ensure that any business associate protects PHI via contractual agreement.

10. Train the workforce
    Consumer Direct will ensure employees are educated on HIPAA, maintaining confidentiality, protecting PHI, and are familiar with the Consumer Direct HIPAA policy.

HIPAA PENALTIES

- $100 civil penalty up to a maximum of $25,000 per year for each standard violated
- Criminal penalties for knowingly disclosing PHI up to a maximum of $250,000

PRIVACY POLICY STATEMENT

Purpose: *The following privacy policy is adopted to ensure that Consumer Direct complies fully with all federal and state privacy protection laws and regulations. Protection of patient privacy is of paramount importance to Consumer Direct. Violations of any of these provisions will result in severe disciplinary action including up to termination of employment and possible referral for criminal prosecution.*

Effective Date: *This policy is in effect as of April 1, 2003; revised March 26, 2013*

Expiration Date: *This policy remains in effect until superseded or cancelled.*

Privacy Officer: *Daryl Holzer (877) 532-8530*

Uses and Disclosures of Protected Health Information

It is the policy of Consumer Direct that protected health information may not be used or disclosed except when at least one of the following conditions is true:

1. The individual who is the subject of the information has authorized the use or disclosure.
2. The individual who is the subject of the information has received our Notice of Privacy Practices and acknowledged receipt of the Notice, thus allowing the use or

disclosure, and the use or disclosure is for treatment, payment or health care operations.

3. The individual who is the subject of the information agrees or does not object to the disclosure, and the disclosure is to persons involved in the health care of the individual.
4. The disclosure is to the individual who is the subject of the information or to the U.S. Department of Health and Human Services for compliance-related purposes.
5. The use or disclosure is for one of the HIPAA "public purposes" (i.e. required by law, etc.).

Deceased Individuals

It is the policy of Consumer Direct that privacy protections extend to information concerning deceased individuals.

Notice of Privacy Practices

It is the policy of Consumer Direct that a Notice of Privacy Practices must be published, that this Notice and any revisions to it be provided to all individuals at the earliest practicable time, and that all uses and disclosures of protected health information are in accordance with Consumer Direct's Notice of Privacy Practices.

Restriction Requests

It is the policy of Consumer Direct that serious consideration must be given to all requests for restrictions on uses and disclosures of protected health information as published in Consumer Direct's Notice of Privacy Practices. It is furthermore the policy of Consumer Direct that if a particular restriction is agreed to, then Consumer Direct is bound by that restriction.

Minimum Necessary Disclosure of Protected Health Information

It is the policy of Consumer Direct that (except for disclosures made for treatment purposes) all disclosures of protected health information must be limited to the minimum amount of information needed to accomplish the purpose of the disclosure. It is also the policy of Consumer Direct that all requests for protected health information (except requests made for treatment purposes) must be limited to the minimum amount of information needed to accomplish the purpose of the request.

Access to Protected Health Information

It is the policy of Consumer Direct that access to protected health information must be granted to each employee or contractor based on the assigned job functions of the employee or contractor. It is also the policy of Consumer Direct that such access privileges should not exceed those necessary to accomplish the assigned job function.

Access to Protected Health Information by the Individual

It is the policy of Consumer Direct that access to protected health information must be granted to the person who is the subject of such information when such access is requested, or at the very least within the timeframes required by the HIPAA Privacy Rule. It is the policy of Consumer Direct to inform the person requesting access where protected health information is located if we do not physically possess such PHI but have knowledge of its location.

Amendment of Incomplete or Incorrect Protected Health Information

It is the policy of Consumer Direct that all requests for amendment of incorrect protected health information maintained by Consumer Direct will be considered in a timely fashion. If such requests demonstrate that the information is actually incorrect, Consumer Direct will allow amending language to be added to the appropriate document and this addition will be done in a timely fashion. It is also the policy of Consumer Direct that notice of such corrections will be given to any organization with which the incorrect information has been shared.

Access by Personal Representatives

It is the policy of Consumer Direct that access to protected health information must be granted to personal representatives of individuals as though they were the individuals themselves, except in cases of abuse where granting said access might endanger the individual or someone else. We will conform to the relevant custody status and the strictures of state, local, case, and other applicable law when disclosing information about minors to their parents.

Confidential Communications Channels

It is the policy of Consumer Direct that confidential communications channels be used, as requested by the individuals, to the extent possible.

Disclosure Accounting

It is the policy of Consumer Direct that an accounting of all disclosures subject to such accounting of protected health information be given to individuals whenever such an accounting is requested.

Marketing Activities

It is the policy of Consumer Direct that any uses or disclosures of protected health information for marketing activities will be done only after a valid authorization is in effect. It is the policy of Consumer Direct to consider marketing any communication to purchase or use a product or service where an arrangement exists in exchange for direct or indirect remuneration, or where Consumer Direct encourages purchase or use of a product or service. Consumer Direct does not consider the communication of alternate forms of

treatment, or the use of products and services in treatment to be marketing. Furthermore, Consumer Direct adheres to the HIPAA Privacy Rule that face-to-face communication with the patient, or a promotional gift of nominal value given to the patient, does not require an Authorization. All marketing activities will be approved in advance by the Privacy Officer.

Judicial and Administrative Proceedings

It is the policy of Consumer Direct that information be disclosed for the purposes of a judicial or administrative proceeding only when: accompanied by a court or administrative order or grand jury subpoena; when accompanied by a subpoena or discovery request that includes either the authorization of the individual to whom the information applies, documented assurances that good faith effort has been made to adequately notify the individual of the request for their information and there are no outstanding objections by the individual, or a qualified protective order issued by the court. If a subpoena or discovery request is submitted to us without one of those assurances, we will seek to notify the individual, obtain his or her authorization, or obtain a qualified protective order before we disclose any information. In no case will we disclose information other than that required by the court order, subpoena, or discovery request. All releases of information for Judicial and Administrative Proceedings must be approved in advance by the Privacy Officer.

De-Identified Data and Limited Data Sets

It is the policy of Consumer Direct to disclose de-identified data only if it has been properly de-identified by a qualified statistician or by removing all the relevant identifying data. We will make use of limited data sets, but only after the relevant identifying data have been removed and then only to organizations with whom we have adequate data use agreements and only for research, public health, or health care operations purposes.

Authorizations

It is the policy of Consumer Direct that a valid authorization will be obtained for all disclosures that are not for: treatment, payment, health care operations, to the individual or their personal representative, to persons involved with the individuals care, to business associates in their legitimate duties, to facility directories or for public purposes. This authorization will include all the mandatory elements and any authorizations generated from outside Consumer Direct will be checked to see if they are valid.

Complaints

It is the policy of Consumer Direct that all complaints relating to the protection of health information be investigated and resolved in a timely fashion. Furthermore, it is the policy of Consumer Direct that all complaints will be addressed to the Privacy Officer who will be duly authorized to investigate complaints and implement resolutions if the complaint stems from a valid area of non-compliance with the HIPAA Privacy and Security Rule.

Prohibited Activities

It is the policy of Consumer Direct that no employee or contractor may engage in any intimidating or retaliatory acts against persons who file complaints or otherwise exercise their rights under HIPAA regulations. It is also the policy of Consumer Direct that no employee or contractor may condition treatment, payment, enrollment or eligibility for benefits on the provision of an authorization to disclose protected health information.

Responsibility

It is the policy of Consumer Direct that the responsibility for designing and implementing procedures to implement this policy lies with the Privacy Officer.

Verification of Identity

It is the policy of Consumer Direct that the identity of all persons who request access to protected health information be verified before such access is granted.

Mitigation

It is the policy of Consumer Direct that the effects of any unauthorized use or disclosure of protected health information be mitigated to the extent possible.

Safeguards

It is the policy of Consumer Direct that appropriate physical safeguards will be in place to reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the HIPAA Privacy Rule. These safeguards will include physical protection of premises and PHI, technical protection of PHI maintained electronically, and administrative protection. These safeguards will extend to the verbal communication of PHI. These safeguards will extend to PHI that is removed from Consumer Direct.

Business Associates

It is the policy of Consumer Direct that business associates must be contractually bound to protect health information to the same degree as set forth in this policy. It is also the policy of Consumer Direct that business associates who violate their agreement will be dealt with first by an attempt to correct the problem, and, if that fails, by termination of the agreement and discontinuation of services by the business associate.

Training and Awareness

It is the policy of this Consumer Direct that all members of our workforce have been trained by the compliance date on the policies and procedures governing protected health information and how Consumer Direct complies with the HIPAA Privacy and Security Rule. It is also the policy of Consumer Direct that new members of our workforce receive training

on these matters within the employee's probationary period time after joining the workforce. It is the policy of Consumer Direct to provide training should any policy or procedure related to the HIPAA Privacy and Security Rule materially change. This training will be provided within a reasonable time after the policy or procedure materially changes. Furthermore, it is the policy of Consumer Direct that training will be documented indicating participants, date and subject matter.

Sanctions

It is the policy of Consumer Direct that sanctions will be in effect for any member of the workforce who intentionally or unintentionally violates any of these policies or any procedures related to the fulfillment of these policies.

Retention of Records

It is the policy of Consumer Direct that the HIPAA Privacy Rule records retention requirement of seven years from the date of discharge will be strictly adhered to. For minors, records will be retained for at least three years after the minor reaches the age of majority. All records designated by HIPAA in this retention requirement will be maintained in a manner that allows for access within a reasonable period of time. This records retention time requirement may be extended at Consumer Direct's discretion to meet with other governmental regulations or those requirements imposed by our professional liability carrier.

Cooperation with Privacy Oversight Authorities

It is the policy of Consumer Direct that oversight agencies such as the Office for Civil Rights of the Department of Health and Human Services be given full support and cooperation in their efforts to ensure the protection of health information within Consumer Direct. It is also the policy of Consumer Direct that all personnel must cooperate fully with all privacy compliance reviews and investigations.

Investigation and Enforcement

It is the policy of Consumer Direct that in addition to cooperation with Privacy Oversight Authorities, Consumer Direct will follow procedures to ensure that investigations are supported internally and that members of our workforce will not be retaliated against for cooperation with any authority. It is our policy to attempt to resolve all investigations and avoid any penalty phase if at all possible.