Orientation Packet
Section VIII
HIPAA Training

Clearwater Office: 28050 US HWY 19 N St 205 ● Clearwater FL, 33761 ● Tampa Office: 6601 Memorial Hwy Ste 106 ● Tampa, FL, 33615 ●Phone: 727-286-8916 ● Fax 727-724-1201 ● Email: AbundantlifeHHA@gmail.com

Abundant Life Home Health Agency Orientation Packet Section VIII

In 1996, Congress enacted the Health Insurance Portability and Accountability Act, also known as HIPAA. Among the primary purposes of HIPAA are (1) to protect people from losing their health insurance if they change jobs or have pre-existing health conditions, (2) to reduce the costs and administrative burdens of healthcare by creating standard electronic formats for many administrative transactions that are currently carried out on paper, and (3) to develop standards and requirements to protect the privacy and security of confidential healthcare information.

Recently, the Department of Health and Human Services issued new regulations referred to as the Privacy Rule and Security Rule. The regulations require healthcare organizations to adopt processes and procedures to ensure the highest degree of patient confidentiality. These processes include administrative, physical and technical safeguards to ensure that medical information is stored, transmitted and received in a safe and secure manner.

As you can imagine, the HIPAA regulations impact virtually every department of every entity that has access to confidential health information. Hospitals, medical practices, insurance companies, medical-device manufacturers and other healthcare organizations are undergoing major changes in the way they handle patient information.

The Privacy and Security Rules provide stiff penalties for those who fail to comply with the requirements or who improperly disclose or misuse protected health information (PHI). It is important that all who may come into contact with PHI understand and carry out their responsibilities under the Rules, as outlined in this training program.

HIPAA is a broad and far-reaching law. Entities covered by the Privacy and Security Rules include healthcare plans, providers and clearinghouses.

The Rule also extends to the business associates of covered entities, which include auditors, consultants, lawyers, data and billing firms, and others with whom the covered entities have agreements involving the use of protected health information. The covered entity must receive satisfactory assurances that the business associate will comply with the Privacy and Security Rules, though

the covered entity need not monitor the business associate's work unless it learns of a problem with compliance. You do not need a business associate agreement for employees, cleaning services, and contracted employees such as a physical therapist who perform a substantial portion of their work for this agency. The Privacy Rule requires the return or destruction of all protected health information (PHI) at the termination of a business associate agreement contract only where feasible or permitted by law.

In addition, the Rules apply to any company that offers healthcare and treatment to its employees on-site. Thus, if an employer or school operated an on-site clinic, the clinic would be a covered entity, and its patient information would be subject to the Privacy and Security Rules.

Entities Covered by State Law

When covered entities use or transmit protected health information in any form, they must comply not only with the Privacy and Security Rules, but also with any state laws regarding privacy of medical records. In the event of a conflict between HIPAA and state law, HIPAA preempts state law unless the state law is more strict. (In other words, whichever provides greater protection to patients must be followed.)

HIPAA establishes a single set of transaction standards for electronic healthcare transactions, thus enabling healthcare providers and insurance companies to communicate more fluidly. The Privacy and Security Rules cover the following types of information transactions:

1. Healthcare claims (professional, institutional and dental);

2. Health plan eligibility inquiries and responses;

3. Enrollment and disenrollment in a health plan;

4. Healthcare payment and remittance advice;

5. Health plan premium payments;

6. Claim status inquiries and responses;

7. Referral certification and authorization; and

8. Coordination of benefits.

The Rules also require covered entities to use special coding standards for all transactions involving electronic data interchange (EDI), including the use of "unique identifiers" for providers, health plans, employers and patients. These new coding standards are still being developed and refined by the Department of Health and Human Services.

The Privacy and Security Rules protect individually identifiable health information
transmitted or maintained by a covered entity, no matter what form it takes.

That means that when a doctor takes notes in a medical chart, when a hospital data-entry clerk types health insurance information into a computer, or when healthcare providers discuss a patient's condition, any identifiable health information becomes protected health information (PHI) under HIPAA. Medical records are protected health information. Patients and authorized patient representatives are allowed access to their medical records. The patient can authorize a person to receive PHI information at any time and may also revoke authorization at any time. The need to provide in writing the person(s) that they wish to allow access to PHI. If a patient wants to request a restriction on the disclosure of his/her protected health information it must be in writing. However, the patient may request to review their records in person and are not required to provide the request in writing.

When a patient requests access to his/her medical records you can provide a summary if you think it is too difficult for the patient to interpret. You must have the requestor agree on charges for the summary in advance. When a patient requests copies of his/her medical records you can charge reasonable cost-based fees for providing the copies/summaries.

Note, however, that employment records held by a covered entity in its role as an employer are not considered PHI.

While many covered entities may seek to rely on practice-management software or healthcare clearinghouses as a means of ensuring HIPAA compliance for their healthcare transactions, software alone cannot provide a complete solution. Most of the work in complying with HIPAA for all covered entities is in developing and administering systems and policies that prevent the misuse of PHI in a comprehensive and consistent way. This agency has 60 days to respond to a request to amend a record. The agency can refuse to make amends in certain cases.

The Privacy Rule requires a covered entity to:

- Provide patients with a Notice of Privacy Practices (NPP); and

- Make a good-faith effort to obtain a patient's written acknowledgment of receiving the NPP.

The NPP must inform patients of (1) the uses and disclosures of PHI that the entity may make, (2) the patient's right to access and amend their medical information, and (3) the covered entity's responsibilities with respect to PHI. Notice of Privacy Practices (NPP) must be given to each patient at the first visit after April 13, 2003, posted on the company Web site, if it has one, and posted in the office. If I forget to give a Notice of Privacy Practices (NPP) to a patient, I have to mail it on the date of service and document my actions. The agency can make changes to the NPP if it has reserved the right in the notice.

Once it has obtained the acknowledgment or has made a good-faith effort to do so, the entity may:

- Use PHI for its own treatment, payment or healthcare operations; and

- Disclose PHI to other covered entities for their treatment, payment or certain limited healthcare operations.

When using or disclosing PHI or when requesting PHI from another covered entity, a covered entity must make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use or disclosure.

As a general rule, a covered entity may not use or disclose protected health information for purposes other than treatment, payment and healthcare operations without the patient's written authorization. A copy of an authorization is acceptable if all elements are included.

Marketing

The Privacy Rule prohibits a covered entity from disclosing PHI to others for marketing purposes without the patient's written authorization. For example, a pharmacy may not provide a pharmaceutical company a list of patients with a particular disease or condition in order for the pharmaceutical company to market drugs to those patients without their authorization.

At the same time, communications regarding treatment, case management or the recommending of alternative therapies are excluded from the definition of "marketing," as are communications that promote health in a general manner. Thus, for example, a health- related newsletter that a covered entity distributes to patients to inform them about new healthcare developments would not be considered marketing under the Privacy Rule.

Incidental Disclosures

The Privacy Rule allows "incidental" disclosures of PHI, as long as the covered entity uses reasonable safeguards and adheres to the "minimum necessary" standard. For example, doctors' offices may use waiting-room sign-in sheets, hospitals may keep charts at bedside, doctors may talk to patients in

semi-private rooms, and medical staff may confer at the nurse's station without violating the Privacy Rule.

Since many of us receive, store and transmit PHI as part of our day-to-day responsibilities, The Privacy Rule requires the following administrative safeguards to ensure that PHI is not compromised:

1. Designating a Privacy Officer to be responsible for the development and implementation of privacy policies;

2. Providing physical safeguards to protect our computer systems and related equipment from fire, other environmental hazards and intrusion;

3. Using technical safeguards like encryption software to transmit health information over the Internet;

4. Requiring business associates (lawyers, consultants, auditors, billing companies, pharmacists, etc.) to confirm that they will protect PHI;

5. Developing a system to track who accessed what information; and
6. Implementing rules for addressing violations of privacy, security and transaction regulations, including establishing a process for making complaints and preventing retaliation against anyone who reports a HIPAA violation. The patient may lodge a complaint to any staff member or the regulatory body.

7. If the Secretary of Health and Human Services (HSS) validates a complaint: It may result in a compliance review.
8. If a non-authorized disclosure of protected health information (PHI) is made: You must keep a record of this for six years and give the patient a full accounting upon proper request.

Employees must receive an initial training on HIPAA and also requires those with access to PHI to undergo periodic training on these and other appropriate privacy procedures, and to keep documented proof that these trainings have been given. Everyone who works in my office, including unpaid volunteers,

contract employees, and casual laborers, must be trained or show documentation of training about HIPAA

A privacy officer should conduct the following steps:

- Identify the internal and external risks of disclosure of protected health information (PHI)
- Create and implement a plan to reduce the risk of releasing PHI in those areas identified
- Train all personnel on the practice's privacy and security of PHI.
- Monitor the implementation and enforce appropriately any breaches of policy.

The Security Rule also requires that administrative, physical and technical safeguards are in place to prevent the improper use or disclosure of PHI. The required administrative safeguards are as follows:

- Certification Review: A technical evaluation to ensure that our computer environment is secure from intrusion.

- Chain of Trust Agreements: Agreements with external recipients of PHI confirming that they will protect the confidentiality of data exchanged.

- Contingency Plan: A plan for responding to system emergencies, including the performance of backups, emergency-mode operations, and disaster-recovery procedures.

- Policies & Procedures: Policies and procedures for the proper use of healthcare information.

- Access Controls: A plan for granting different levels of access to healthcare information, including policies that determine each individual's right to access the information.

- Internal Audit Procedures: An in-house review of system activity records (such as log-ins, file accesses, and security incidents).

- Personnel Security: Security checks and special training for all employees with access to sensitive information regarding the proper use and handling of PHI, and documentation to verify that the training has occurred.
- Security Configuration Management: Procedures for the security of our computer systems, such as virus checking and security testing.

- Security Incident Procedures: Instructions for reporting security breaches.

- Security Management Process: A process to ensure that we have the proper infrastructure in place to prevent and detect security breaches.

- Termination Procedures: Procedures to prevent a terminated employee from having access to confidential information.

HIPAA also requires those with access to PHI to undergo periodic training on these and other appropriate security procedures, and to keep documented proof that these trainings have been given.

The Security Rule also requires a number of physical steps to ensure that PHI contained in computers is properly protected from fire and environmental hazards, as well as from intrusion. Physical safeguards include the following:

- Security Management: Assignment of responsibility for Security management.

- Media Controls: A set of procedures that govern the receipt and removal of hardware and software (such as diskettes, tapes, and personal data assistants).

- Physical Access Controls: Procedures that deter intruders from accessing environments where sensitive information resides.

- Equipment Controls: Security policies for bringing hardware and software into and out of offices, including policies on how to dispose of hardware and other storage media.

- Guidelines on Workstation Use: Procedures describing the proper functions to be performed on computers, and how to handle sensitive information that may be displayed on computer screens.

Finally, the Security Rule requires certain technical safeguards for PHI, including:

- Access Controls: Controls to ensure that access to sensitive information is available on a need-to-know basis, based on roles and context.
- Audit Controls: Controls to record and examine system activity, helping to eliminate unnecessary access to sensitive information.

- Authorization Controls: Controls for obtaining consent for the use and disclosure of health information.

- Data Authentication: Controls to help ensure that health data has not been altered in an unauthorized manner.

- Entity Authentication: Controls to ensure that data is sent to the intended recipient and received by the intended party. These controls include the use of password protections, PIN numbers and, when sent over public networks, encryption.

Sending PHI via E-mail and Fax

According to the Security Rule, it is permissible to use the Internet to transmit PHI, as long as (1) an acceptable method of encryption is used to protect confidentiality, and (2) appropriate authentication procedures are followed to ensure correct identification of the sender and receiver. Although faxes are transmitted over telephone lines, they are not considered to be "covered transactions," so they may be sent without additional security precautions.

The HIPAA regulations take effect for covered entities on April 14, 2003, while various parts of the Security Rule go into action between now and April 2005. Failure to comply with the Privacy or Security Rule can lead to significant financial and other penalties:

- Civil monetary penalties for each individual failure to comply with HIPAA provisions include a fine of $100 for each violation with a cap of $25,000 per year for multiple violations of the same provision.

- Criminal penalties for a basic offense include fines of up to $50,000 and/or imprisonment for up to one year.

- Criminal penalties for an offense committed under false pretenses include fines of up to $100,000 and/or imprisonment of up to five years.

- Criminal penalties for an offense committed with the intent to use PHI for one's commercial advantage include fines of up to $250,000 and/or imprisonment of up to ten years.