HIPAA ORIENTATION CHECKLIST

WHO:

- Protection
- Compliance
- Enforcement

WHY:

Reason for HIPAA

WHEN:

Compliance Date

WHERE:

HIPAA Applications

WHAT:

- Privacy Rule
- Uses & Disclosures
- Transaction Rule
- Security Rule
- Non-Compliance Penalties

HOW:

- Visible PHI
- Medical Records
- Fax Machines/Faxes
- Shredding PHI
- Patient Discussion in Public
- Confidential Conversations
- Patient Phone Usage
- Telephone Conversations that Include PHI
- HIPAA Software Compliance
- Computer System Firewall

Computer:

- Visibility
- Passwords
- Log on/off
- Email Confidentiality Statement

_____

Contractor Name (Print)

_____ _____

Contractor *Signature* Date

_____ _____

Oriented By (Agency Representative) Date

HIPAA - The 5 Ws and How
For Field Staff

Who?

What?

Where?

When?

Why?

How?

HIPAA - The 5 Ws and How

WHO?

Who passed HIPAA?

The HIPAA standards were passed into law by Congress and President Bill Clinton signed them into law. The Transactions Rule was passed by Congress and signed into law by President George W. Bush.

Who is protected by HIPAA?

Title I protected people who had lost or changed their jobs from losing their health insurance. It is the centerpiece of the HIPAA legislation.

Title II protects patient health information and gives patients more control over and access to their health information.

Who must comply with HIPAA privacy standards?

There are several COVERED ENTITIES, one of which is the health care facility and staff and those with whom it does business.

Who will enforce HIPAA?

Depending on which Standard the Agency is out of compliance on, it will be either the Health and Human Services Office for Civil Rights or the Centers for Medicare and Medicaid.

HIPAA - The 5 Ws and How

WHAT?

What is HIPAA?

As it pertains to a health care facility, HIPAA is intended to protect the privacy of people receiving health care if the provider of that care conducts even one covered transaction electronically. The covered transactions include processing health care claims for billing and payments, as well as coordination of benefits.

What is the Privacy Rule?

Essentially, the Privacy Rule is intended to give individuals a level of protection of their individually identifiable health information and to provide more control over how their health information is used and disclosed. The Protected Health Information (PHI) is electronic, paper, or oral information related to an individual's health condition that is found in:

- ☐ patient medical records
- ☐ patient billing records
- ☐ databases
- ☐ formal and informal discussions

The identifiers included in PHI of the individual, his/her relatives, employers, or household members include:

- ☐ name
- ☐ postal address information other than town/city, state and zip code
- ☐ telephone number
- ☐ fax number
- ☐ electronic mail address
- ☐ social security number
- ☐ medical record number

- ☐ health plan beneficiary number
- ☐ account number
- ☐ certificate/license number
- ☐ vehicle identifiers and serial numbers, including license plate numbers
- ☐ Web Universal Resource Locators (URLs)
- ☐ Internet Protocol address numbers
- ☐ biometric identifiers such as fingerprints or voice prints
- ☐ full face photographs or other comparable images
- ☐ diagnoses
- ☐ treatment

What are the permitted uses and disclosures of PHI?

An agency can use PHI for:

- ☐ treatment, payment and health care operations
- ☐ treatment activities of any health care provider
- ☐ for payment activities of the entity to which PHI is disclosed
- ☐ for the health care operations of another covered entity if
  - ☐ both the agency and the other covered entity has or has had a relationship with the individual and the PHI pertains to that relationship, i.e., the doctor's office, the lab, the therapist
  - ☐ the disclosure is for specified health care operations purposes including quality assessment and improvement activities, case management or care coordination, training, accreditation activities, licensing activities, fraud and abuse detection, research, public health and in emergencies affecting life or safety, judicial proceedings, to provide information to the next-of-kin, for identification of the body of a deceased person, and compliance

In all instances, the agency must make reasonable efforts to limit the PHI used, disclosed, or requested to the minimum amount necessary. This also means the agency must decide the minimum amount of PHI needed by employees to perform their duties. The exception is that it does not apply to a disclosure made for treatment purposes.

HIPAA - The 5 Ws and How

WHERE?

Where do I have to apply HIPAA standards?

The easy answer is EVERYWHERE!! Examples include but certainly are not limited to:

- ☐ business office, especially in areas of public access
- ☐ hospitals
- ☐ doctors' offices
- ☐ patient's/client's homes
- ☐ nursing homes
- ☐ assisted living facilities that provide health care services
- ☐ elevators
- ☐ restaurants
- ☐ hallways
- ☐ desks
- ☐ file rooms
- ☐ field staffs' cars and homes
- ☐ staff mailboxes
- ☐ fax machine area
- ☐ conference room
- ☐ agency kitchen
- ☐ agency bathroom - especially if it is a public facility

HIPAA - The 5 Ws and How

WHEN?

When is HIPAA compliance required?

There are different dates for the different HIPAA standards. The date we are focusing on now for the privacy standard is **April 14, 2003**.

HIPAA - The 5 Ws and How

WHY?

Why was HIPAA passed?

One of the reasons for passing HIPAA was to protect people who had lost or changed their jobs from losing their health insurance.

Other reasons included:

- ☐ to assist health care entities to use technology more efficiently by providing uniform, national standards for submitting electronic transactions
- ☐ to establish a nationwide, minimum level of protection of patient health information
- ☐ to give a level of protection to individuals' privacy and to provide them with more control over how their health information is used and disclosed while giving them more access to their files

Why does the agency have to comply with HIPAA?

- ☐ to avoid fines and penalties
- ☐ avoid unwanted attention should agency be reported
- ☐ ensure patient/client satisfaction
- ☐ IT'S THE RIGHT THING TO DO

HIPAA - The 5 Ws and How

HOW?

How can I be sure I'm compliant with HIPAA?

- ☐ Familiarize yourself with the HIPAA regulation
- ☐ When you visit the office:
  - ☐ Is PHI visible on white boards, desks, by copier, by fax machine, on computer screens?
  - ☐ Are medical records stored in a record room or file cabinets?
- ☐ Do you have travel charts with PHI that you take off premises?
  - ☐ How is PHI protected?
  - ☐ Is it visible in the car?
  - ☐ Do you take it into the patient's/client's home?
  - ☐ What happens if it gets lost?
  - ☐ What happens to PHI in the travel chart when it is no longer needed?
- ☐ Do you have a fax machine at your home office?
  - ☐ Who has access to faxes?
- ☐ Do you send PHI via fax?
  - ☐ How are you sure it is sent to and received by the correct recipient?
  - ☐ Is there a confidentiality statement on the cover page?
- ☐ Do you use paper that has PHI on it as scrap paper or use the other side in the fax machine or copier?
- ☐ Do you shred PHI that is no longer needed?
- ☐ When you visit the office do you discuss patients' PHI in public places such as the kitchen, bathroom, elevator?
- ☐ Do you call out to others in the office about patients?

- ☐ Do you use an intercom system?
- ☐ Do telephone conversations that include PHI such as taking orders or scheduling take place in private areas away from where visitors or other patients are?
- ☐ Do you use a patient's/client's phone to make calls about other patients such as to a doctor's office?
- ☐ How do you authenticate who you are talking to on the phone before disclosing PHI?

What are the penalties for non-compliance?

Currently there is no case law for HIPAA compliance. It remains unclear how it will be enforced. It is known that if a privacy violation is reported and substantiated, there could be civil or criminal penalties.

- Civil Penalties
  $100 per incident up to a maximum of $25,000 per person, per year, per standard

- Criminal Penalties
  - up to $50,000 and one year in prison for obtaining or disclosing PHI
  - up to $100,000 and up to five years in prison for obtaining PHI under false pretenses
  - up to $250,000 and up to 10 years in prison for obtaining or disclosing PHI with the intent to transfer, sell, or use it for monetary gain or malicious harm.

You can see how important it is to make reasonable efforts to protect your patient's/client's health information. You've been doing it under the concept of confidentiality but now the rules are even stricter.

SAMPLE CONFIDENTIALITY STATEMENTS

FAX

The documents accompanying this fax transmission contain confidential information belonging to the sender that is legally privileged. This information is intended only for the use of the individual or entity named above. The authorized recipient of this patient information is prohibited from disclosing the information to any other party. If you have received this transmission in error, please notify the sender immediately and destroy the information that was faxed in error, and keep any information you may have viewed confidential.

E MAIL

This e-mail transmission and any attachments contain confidential information belonging to the sender, which is legally privileged. The information is intended solely for the use of the individual(s) or entity addressed. If you are not the intended recipient, you are hereby notified that any copying, disclosure, distribution, or use of this e-mail and/or attachment is strictly prohibited. If you received this transmission in error, please delete it from your computer system and notify (*the sender*) at (*sender's e-mail address*).

OR

Please be aware that this e-mail transmission is not guaranteed to be 100 percent secure from hackers. Be aware that others could possibly read what is in this e-mail. We have done what we can to keep our e-mail transmissions secure but do need to caution both parties of this possible security breach with confidential information. If you have any questions, please contact the sender of this e-mail.