



WHAT IS HIPAA?

- **HIPAA** stands for Health Insurance Portability and Accountability Act

The Purpose of HIPAA is.....

- To protect and enhance the rights of consumers by providing them/us access to their/our health information and controlling inappropriate use of the information.
- To improve the quality of healthcare in the US by restoring trust in the healthcare system among consumers, healthcare professionals and the multitude of organizations and individuals committed to the delivery of care.

The Basics of the Legislation:

- To improve access to health insurance
- To reduce fraud and abuse
- To increase efficiency and effectiveness of the healthcare system
- To establish standards for accessing, storing and transmitting medical data and ensuring security and privacy of protected health information (PHI)

HIPAA Has Five Components:

- Title I: Healthcare Access, Portability and Renewability
- Title II: Preventing Healthcare Fraud and Abuse; Administrative Simplification; Medical Liability and Reform
- Title III: Tax Related Health Provisions
- Title IV: Application and Enforcement
- Title V: Revenue Offset

Who Does it Affect?

- All healthcare organizations. This includes all healthcare providers, insurance plans, and healthcare clearing houses...essentially anyone who transmits health information in electronic form.

How Does HIPAA Affect Me?

- As an employee of Medical Staffing Resource, Inc., your role is to help maintain the privacy and the security of protected health information (PHI) at all facilities in which you work. PHI is considered to be all client records and other identifiable

treatment information used or disclosed in any form, whether electronically, paper, or verbally.

- Keep client information from public view and the view of other clients.
- Protect your password used for any computers to perform your job.
- Also, refrain from discussing client information in public places.

What is the Difference Between Privacy and Security?

Security....is the ability to control access and protect information from:

- Accidental or intentional disclosure to unauthorized persons
- Alteration
- Destruction
- Loss

Privacy....defines who is authorized to access information.

- Individuals have the right to keep information about themselves from being disclosed.
- Clients, parents/guardians, and referral source also have the right to receive written notice of all privacy policies prior to treatment.

What is Confidentiality?

- Confidentiality is the delicate balance between a Medical Staffing Resource, Inc. employee's need to know and the client's right to privacy.
- All Medical Staffing Resource, Inc., employees are obligated to protect client privacy rights. This includes information in any form or media (i.e., electronic, paper, oral, CD, disk).

What Does Protected Health Information (PHI) Include?

- Name
- Photographic images
- Any date (birth date, admit date, discharge date, etc.)
- Social Security number
- Health Plan numbers
- Account numbers
- Treatment plan information (i.e., diagnosis, medications, etc.)
- Address
- Finger prints
- Telephone number
- Email address
- Medical record number
- Any identifying number, characteristic or code

How is Privacy Most Often Violated?

- Discussion of client information in a public place or with inappropriate, unauthorized individuals.
- Paper or electronic information left exposed where visitors, other clients or other unauthorized individuals can view it.
- Records accessed without prior permission.
- Records accessed even though the information is not needed to perform job duties.
- A staff member using another staff member's computer to login or password.
- Unauthorized persons hearing patient sensitive information.

Haven't We Always Had Privacy and Security Policies?

Absolutely! The difference now is that we are being held accountable by the federal government, and our policies may need to be revised to include new federal regulations. There are now fines and possible jail time for breaches in privacy and confidentiality or protected health information (PHI)

When does this start?

The privacy rule was effective April 14, 2001. Compliance is required for the privacy rule on April 14, 2003. After that date, civil and federal penalties can be imposed for knowingly misusing and individual's identifiable health information.

What do I do if I become aware of a privacy or security issue?

- If you become aware of a privacy or security issue, bring the issue to the attention of the facility supervisor **immediately**.

How can I protect a client's privacy?

- Treat all information as if it were about you or your family.
- Access only those systems that you are authorized to access.
- Use only **your own** computer login and password.
- Access only information you need to do your job.
- Only share sensitive and confidential information with others who have a "need to know".
- Refrain from discussing clients in public places.
- Never share your computer login or password.
- Log off your computer when you leave it, (even if it is only for a minute!).
- Close the office door where client information is kept.
- Keep PHI off counter tops, tables and/or out of easily, viewable areas. Turn over client information when not in use, so PHI is not visible to others.
- If displaying client names, use only first name or initials.
- Turn off computer screens so that they are not visible to passersby.

- If folders are in folder bins outside of an office area, turn files/folders so that the patient's name faces the wall and is not easily visible to people walking by.

When can I give someone information about a client?

- When needed by another facility employee to complete an assignment.
- Client information can be released when permitted by law (such as parent/legal/guardian/referral source).
- When there is a release of information form signed by the patient.