

POLICY AND PROCEDURE CONCERNING CONFIDENTIALITY

Appendix A

THINGS YOU NEED TO KNOW ABOUT HIPAA

What is HIPAA?

HIPAA stands for the federal law entitled the Health Insurance Portability and Accountability Act, which was passed in 1996.

Regulations issued under HIPAA that protect the privacy of health information for all Americans go into effect April 14, 2003.

How does HIPAA affect professionals in the MR/DD field?

As professionals in the MR/DD field, we are legally responsible to protect the health information of our consumers. Special laws mandate the ways in which we store and share this information.

All the consumers we work with need to be given a **privacy statement**, which explains how their health information will be used and their rights under this new privacy law.

What information does HIPAA protect?

The HIPAA regulations safeguard **Protected Health Information (PHI)**. Protected Health Information (PHI) includes an individual's:

- Health (Diagnosis)
- Provision of care (Services received)
- Payment of services (How payment will be made)
- Information which identifies the individual (Name, address, social security, etc.)

When can PHI be shared?

Protected Health Information (PHI) may be shared for:

- Treatment (e.g., for day program or residential services, clinic, etc.)
- Payment (e.g., billing for services)
- Health Care Operations (e.g., such as quality assurance, program oversight)

In most instances you do not need consumer consent for these purposes unless you are sharing sensitive information (e.g., HIV/AIDS information, mental health records) that is protected by special state laws.

When sharing information for Treatment, Payment and Health Care Operations, how *much* information may I share?

For the purposes of **payment** and **health care operations** the ***minimum information necessary*** should be shared. For purposes of **treatment** the concept of minimum necessary should not impede the free flow of information necessary to ensure comprehensive treatment.
When do I need a special consent to share PHI?

Under most other circumstances, it would be necessary to get the consent of the consumer or his/her representative to release their PHI. (For example: Marketing, publicity, referrals to non-treatment programs such as recreation, etc.)

In these cases, it is very important to explain carefully to consumers what they are agreeing to and to use the Agency's standard authorization form.

Are there other circumstances where information may be disclosed without consent?

There are a number of possible situations where this information can be disclosed for "public need" purposes without consent. These include, but are not limited to the following:

- Government audits and investigations
- Public health and safety
- A Subpoena from the courts

What are the steps professionals need to take to protect the consumer's PHI?

Discussion: Don't discuss information about consumers in a public place where others can overhear.

Files: Make sure files are not kept where unauthorized people can see them and that they are locked away when not in use.

Fax: When sending a fax, make sure an authorized person is on the other end to receive it.

Computers: All computers should be password protected.
Never share your computer password with anyone else.
Your computer screen should face away from public area/viewing.
When stepping away from a computer in use, you can protect consumer information by:

- Closing all applications
- Using a screen saver (if possible, with password protection)

Do not send PHI by e-mail unless it is encrypted

How do I dispose of documents containing PHI?

Anything containing PHI has to be disposed of in a way that makes the information unreadable. (For example: use a shredder)

If I don't know whether or not to give out information, whom do I talk to?

You should speak to your supervisor or your agency's designated privacy officer.