

Health Information Security*

Adopted & Effective: April 2003

Policy Statement:

It is the policy of Children's Aid and Family Services, Inc. (hereafter referred to as 'the organization') to safeguard and secure the private health information of its clients. The organization understands the importance of blending the privacy requirements with that of the security requirements, and to that end, has established the following basic procedures for ensuring the security of clients' health information, both during and after services have been provided. The organization has also, in recognition of this fact, developed this security policy to include its' workforce commitment to the safeguard and security of clients' information stored in any form within or outside the organization, including information stored in paper and media forms (e.g. computer desk-tops, network/servers, and floppy disks).

Procedure:

1. Paper records, documents containing clients' information will remain locked up at all times. Storage may include, locked file cabinets, locked records room, with limited access by work force members not involved in the treatment and care of clients.
2. The organization's workforce directly involved in the treatment and care of clients' are encouraged to establish a list of other workforce members on the treatment team authorized to have access to client health information. Any workforce member or others not directly involved in the treatment of a client (such as those present or invited to the treatment planning or clinic meeting of a client) and who wishes to access the client's information for reasons other than those required to provide TPO, any only do so if the client's prior authorization has been obtained. A record of such authorization will be maintained in the case record. In practicing this requirement, as with all cases of clients' privacy, workforce members are required to ensure that the "*minimum necessary*" requirement is applied at all times. Thus allow access to only the information required by the person accessing the record or information to carry out a particular activity in relation to the client.
3. Workforce members offices will remain locked at all times when the workforce members are not in the office.

4. Files/records will be stored in such a way that the personal health information of clients, including names will be secure from visitors to the building. And no client record may be left unattended on a workforce member's desk.
5. Workforce members are encouraged not to transport clients' health information in their cars, laptops or outside designated work areas.
6. Each workforce member has individualized password for workstation and network log-on. If your password for any reason does not work, or you don't have one, contact the MIS staff.
7. Active screen savers are enabled on all workstations to restrict unauthorized users from accessing information on the workstation when the computer is idle for a prolonged period of time.
8. With servers and networks in general, privacy and security are very important, not just in preventing outside access, but also the restriction of those in other departments from accessing information intended only for certain individuals or departments. To that end department level permissions have been granted to workforce members'.
9. Diskettes (or "floppy disks") containing client information may not be taken outside the organization or shared with unauthorized persons. Since the organization recognizes that diskettes can contain viruses, workforce members may not to bring a disk home for use in the office. As much as possible, workforce members are encouraged to use the network servers instead of diskettes, in storing and updating client information, since these are continually checked for virus attack.
10. Workforce members working in the group homes, will adopt steps that will ensure the security and privacy of individual client information from other clients in the home, including, not having leaving individual records or health information unattended in staff offices or clients' and/or common areas in the home.
11. When allowing clients' access to computers/workstations in the group homes, adequate steps must be taken to ensure that files containing residents' health information are not accessible to residents.
12. Other security measures as deemed appropriate to safeguard clients' information.

**Please note that this policy may be revised in future to reflect changes made to the final 'HIPAA Security Rule'.*

