TN Department of Children's Services

POLICY

9.4 Confidential Client-Specific Information	
Application: To All Department of Children's Services Employees and Contract Service Providers	
Authority: TCA 36-1-125, 36-1-126; 37-1-153; 37-1-409; 37-1-612; 37-2-408; 37-5-105 (3); 37-5-106; 37-5-107	**Standards: COA**: PA-CR2, PA-RPM 2.01(f), PA-RPM 6, PA-TS 2.02
Commissioner:	**Date:**
Original Effective Date: 07/01/00 Current Effective Date: 01/30/15	Supersedes: DSC 9.4 08/15/11 Last Review Date: 01/30/15
Glossary: None	

Policy Statement:
The Department of Children's Services shall ensure that all information obtained, created or data collected, directly or indirectly, in any medium, which identifies a client, will be kept confidential in order to protect their privacy. Client case files and related information are official records which have been designated confidential by law and will be safeguarded in accordance with applicable statutes, rules, policies, and ethical standards.

Purpose:
To establish guidelines to ensure that client- specific information is kept confidential and to inform clients of DCS of their right to privacy.

Procedures:

A. Office confidentiality

1. Clients have the right for their information to be kept confidential.
   - **a)** To ensure clients have access to knowledge of this and other rights to which they are entitled, Clients Rights information will be posted in the lobby of each DCS office.
   - **b)** The Clients Rights information will be placed in a visible location, clearly marked for easy visibility, and will be posted in English and Spanish.
   - **c)** In areas where more than 3% of the service population speak a language other than English or Spanish as the primary language, the Clients Rights information will also be posted in that language.

Note: Regional Title VI coordinators oversee compliance efforts in the field.

2. All identifiable client information must be maintained in a confidential manner **at all times.**
   - **a)** Staff will hold face-to-face conversations with clients in a private location in the office. In situations where face-to-face conversations take place outside of the office setting, DCS staff must take reasonable measures to safeguard the confidentiality of information being shared by the client.
   - **b)** When making telephone calls from a cubicle or having necessary conversations with other staff members (including case conferences between supervisors and case managers) outside of a private room, staff will use quiet voices and attempt to avoid using identifiable information during the conversation.

B. Safeguarding of confidential information

1. Paper

All case files will be properly labeled according to policy and marked "Confidential". Case files will be kept in a locked location at all times except when in use by staff. as outlined in DCS policies ***9.3 DOE, Youth Education Records***; ***14.11, Child Protective Services Case File Organization, Documentation and Disposition***; ***31.5, Organization of Family Case Files***, and applicable ***DCS Health Insurance Portability and Accountability Act of 1996 (HIPAA) policies-Chapter 32***. Files that are maintained in a file room will be logged in and out of the file room according to the file room procedures posted in each DCS office. See DCS Policy ***9.6 Organization and Maintenance of DCS File Rooms*** for more information.

- **a)** Where lockable storage is not available, other reasonable measures must be taken to safeguard confidential information.
  - ♦ Confidential record information will be maintained in secure shelf/cabinet/storage areas or stored in computers that possess "built-in" security features to prevent access by unauthorized users.
  - ♦ When leaving an office area/desk, all staff will lock up confidential material.
- **b)** All pending, open, or closed client case file record information will be maintained in secure conditions that guarantee confidentiality, integrity, and availability to authorized individuals and agencies when needed. Reasonable precautions, including safeguards from tampering, theft, fire or water damage, environmental hazards, and natural disasters, will be initiated.

2. Visual/electronic

- **a)** DCS staff must ensure that observable confidential information on computer screens is adequately shielded from unauthorized disclosure. Suggested means for ensuring this protection include:

- Use of polarized screens or other computer screen overlay devices that shield information on the screen;
- Placement of computers out of the visual range of persons other than the authorized user;
- Clearing information from the computer screen when not actually being used;
- Locking the computer screen to prevent unauthorized access when leaving the office/desk area; and
- Other effective means as available.

b) DCS staff must safeguard and provide minimum necessary access to confidential information in any format or medium located on:

- Desks;
- Fax machines;
- Photocopy machines;
- Scanners
- Desktop phones with instant messaging capabilities
- Portable electronic devices (e.g., laptop computers, cell phones, smart phones, tablet computers, etc.);
- Computer printers;
- Removable media (e.g., diskettes, CDs, DVDs, flash drives, etc.); and
- Common areas (e.g., break rooms, cafeterias, restrooms, elevators, etc.).

Note: When printing confidential information. All staff members will use the confidential print feature

c) Confidential information will not be sent via text messages on cell phones or smart phones.

C. Release of information

The release of confidential information of a child and his/her family shall be in accordance with DCS Policies ***9.5, Access and Release of Confidential Child-Specific Information*** and ***20.25 Health Information Records and Access.***

D. Record security and recovery

1. Information backups are essential in the event of an emergency or disaster. Therefore, DCS management will ensure that cost effective record security, disaster preparedness and recovery procedures are prepared, implemented, and reviewed annually.

2. The security and recovery of open, inactive, and closed automated client record data will be at the direction of the DCS Office of Information Technology (OIT) based on information owner/user feedback and applicable Records Disposition Authorization (RDA).
3. Formalized security controls and procedures for sensitive and privileged child data provided in electronic communication systems, such as e-mail and the Internet, will be coordinated by DCS OIT.
4. DCS will also comply with federal regulations, court mandates, legal settlements, and accreditation standards concerning the confidentiality of child specific record information.

E. Records disposition

1. Confidential health/medical, educational, foster care, adoption, and CPS record information will be maintained in accordance with the applicable RDA.
2. All other contents such as social histories, face sheets, permanency plans, psychological reports by other agencies, incident reports, court orders, police records, photographs, and any other confidential record not specified for retention will be removed and held in a secured location pending proper destruction.
3. Confidential electronic files will be maintained in accordance with the applicable RDA.
4. Child health/medical and educational records are vital components of the case record and may be maintained separately, regardless of media, in other appropriate and secure areas within DCS facilities, in accordance with applicable RDA and DCS policies.
5. DCS will secure an appropriate media format for any confidential record mandated by statute for preservation, such as sealed adoption files.
6. Retaining records after the expiration of their retention period for the sole purpose of convenience will jeopardize the credibility of the department records retention program. Therefore, DCS will not retain confidential information that duplicates other "official" records, such as birth/death certificates, social security cards, etc., maintained permanently by other governmental entities. No records will be maintained beyond their retention period unless authorized to do so by DCS Legal Counsel.

F. Records destruction

1. Secure storage, timely retention, and proper disposal of confidential record information will be handled in accordance with applicable RDA and DCS policies.

2. Files and documents awaiting disposal or destruction in desk-site containers, lockable storage rooms, or centralized waste/shred bins, will be appropriately labeled and destroyed on a regular basis consistent with record retention requirements.
3. DCS workplaces that do not have lockable storage rooms or centralized waste/shred bins must implement reasonable procedures to minimize access to confidential information.
4. The approved method for destroying confidential paper record information is shredding. Electronic records will be irreversibly destroyed in accordance with state approved methods.
5. DCS Management will be notified regarding any destruction of records. Contact your DCS Records Management Representative for your coverage area.

G. Records Under Litigation Hold

The RDAs and records destruction policy contained in Sections E. and F. above, do not apply to records, whether electronic or in hard copy, that are under a Litigation Hold issued by the DCS General Counsel's Office or the Tennessee Attorney General's Office.

Forms:

None

Collateral Documents:

DCS Health Insurance Portability and Accountability Act of 1996 (HIPAA) policies-Chapter 32.

9.3 DOE, Youth Education Records

9.5, Access and Release of Confidential Child-Specific Information

14.11, Child Protective Services Case File Organization, Documentation and Disposition

20.25 Health Information Records and Access

31.5, Organization of Family Case Files