Department of Children's Services

POLICY

32.1 General Health Insurance Portability and Accountability Act Privacy Requirements	
Application: To All Department of Children's Services Employees	
Authority: Health Insurance Portability and Accountability Act (HIPAA) of 1996; TCA 37-5-105, 37-5-106;	**Standards: COA:** PA-RPM 6
Commissioner:	**Date:**
Original Effective Date: 09/01/07 Current Effective Date: 11/07/17	Supersedes: DCS 32.1 12/15/09 Last Review Date: 11/07/17
Glossary: None	

Policy Statement:
The Department of Children's Services shall comply with the Health Insurance Portability and Accountability Act 1996 (HIPAA) Privacy Rules that establishes minimum Federal standards for protecting the privacy of individually identifiable health information.

Purpose:
To outline procedures for compliance with the HIPAA Privacy Rule for the establishment of a HIPAA program.

Procedures:

A. Appointment of DCS Privacy Officer

1. DCS maintains the designation of an individual as the DCS Privacy Officer who is responsible for the development and implementation of departmentwide policies and procedures relating to the HIPAA requirements to ensure compliance with the federal regulations. The Department Privacy Officer shall be responsible for, but not limited to, the items listed below:
   - **a)** Overseeing all ongoing activities related to the development, implementation, maintenance of, and adherence to the department's policies concerning privacy;
   - **b)** Monitoring the process for receiving, documenting, tracking, investigating, and taking action on all complaints;
   - **c)** Ensuring that DCS is in compliance with its privacy practices and HIPAA privacy policies for all employees; and

d) Training, as applicable.

2. **Regional/Facility Privacy Officers** - At least one individual in each Regional Office and a Youth Development Center serves as support for the Department Privacy Officer and their region or facility.
3. Regional and Facility Privacy Officer designee's are responsible for providing information about privacy practices for their region or facility and coordinating with the Departmental Privacy Officer to assist in the investigation of complaints and processing of client requests.
4. The DCS Customer Relations Unit shall receive, document, track and relay findings on all complaints and requests related to client privacy rights. This office is responsible for establishing and administering a process for receiving and processing all client requests pursuant to DCS Policy, ***32.2 Client Privacy Rights***.
5. In the event there is a breach of confidentiality, DCS must, without unreasonable delay and no later than sixty (60) calendar days after discovery of the breach, notify each individual whose unsecured protected health information (PHI) has been or is reasonably believed to have accessed, acquired or disclosed as a result of the breach. If the unsecured PHI of more than 500 State residents has been or is reasonable believed to have been accessed, acquired or disclosed, notice must be provided to prominent media outlets serving the State. When a business associate discovers a breach, the business associate must notify the covered entity. In all cases of breach, notice must be provided to the Secretary of Health and Human Services (HHS), who will publish on the internet the instances of breach involving 500 or more individuals.

B. Training

1. DCS provides training to all DCS employees on HIPAA privacy practices, rules and regulations.
2. All DCS HIPAA Business Associates are required to provide HIPAA training for their own employees.

C. Safeguarding confidential PHI about clients

1. All DCS employees and business associates respect and protect the privacy of records and health information about clients who request or receive services from DCS.
2. All health information regarding DCS clients is confidential and must be safeguarded in accordance with DCS HIPAA privacy policies and procedures as well as DCS Policies ***9.4, Confidential Child-Specific Records Information*** and ***9.5,***

Access and Release of Confidential Child-Specific Information and ***32.4, HIPAA Administrative, Technical and Physical Safeguards.***

3. DCS and its Business Associates shall not use or disclose PHI unless:
   a) The client has authorized the use or disclosure in accordance with DCS Policy, ***32.3, Uses and Disclosure of Client Protected Health Information***; or
   b) The use or disclosure is specifically permitted under DCS Policy, ***32.3, Uses and Disclosure of Client Protected Health Information.***

D. Conflict with other requirements regarding privacy and safeguarding

1. If any State or Federal law or regulation, or order of a court having appropriate jurisdiction, imposes a stricter requirement upon any DCS policy regarding the privacy or safeguarding of information, DCS shall act in accordance with that stricter standard.
2. All DCS staff act in accordance with established policies and procedures as outlined in DCS Policies, ***9.4, Confidential Child-Specific Records Information*** and ***9.5, Access and Release of Confidential Child-Specific Information*** regarding the safeguarding and confidentiality of individual information, whether health-related or not, in all DCS programs, services and activities.
3. The DCS Privacy Officer must be consulted if there are clarifications needed with privacy policies.

E. DCS Notice of Privacy Practices

1. DCS Staff must give a copy of the ***DCS Notice of Privacy Practices (CS-0699 – Pages 1-3)*** to any client age twelve (12) years old or older enrolling in or receiving services from DCS, describing the actions a client may take, or request DCS to take.
2. Each client who receives services from DCS must sign an acknowledgement form ***CS-0699 DCS Notice of Privacy Practices and Client Acknowledgment (Page 4)***, on their first date of service. This signed acknowledgement is maintained in the client's file for a minimum of six (6) years.
3. If DCS staff cannot acquire a signed acknowledgement from the client, the reason is documented in the client's current child care information system case recordings using the "*Correspondence contact*" type. This signed acknowledgement or documentation of good faith effort is maintained on file for six (6) years.
4. DCS may be considered a business associate of service providers. If so, PHI may be shared among business associates and covered entities without further consent from the individual.

5. The DCS Notice of Privacy Practices contains all information required under federal regulations regarding the Notice of Privacy Practices for PHI under HIPAA.

F. Process for receiving HIPAA complaints

All timeframes for responding to HIPAA complaints shall be in accordance with DCS policy ***32.2, Client Privacy Rights***, Section G.

1. All complaints are forwarded to the DCS Customer Relations Unit. Complaints may be received from:
   - **a)** Parents/guardians
   - **b)** Employees
   - **c)** Providers
   - **d)** Stakeholders
2. All complaints are received/reviewed regardless of format (i.e., personal visits, letters, faxes, telephone or by e-mail, etc.).
3. The DCS Customer Relations Unit immediately contacts the DCS Privacy Officer, RA, regional or facility HIPAA privacy officer regarding the complaint and follow-up with an e-mail to request that an investigation begin with the complaint. The status of the investigation will be provided to the DCS Customer Relations Unit .
4. The regional privacy officer and DCS Privacy officer work in collaboration so that the investigation follows HIPAA rules, guidelines and DCS Policy.
5. The region/facility privacy officer informs the DCS Customer Relations Unit and DCS Privacy Officer of the findings of the investigation.
6. The DCS Customer Relations Unit sends a final written communication of the findings from the investigation. This communication will also inform the person of their rights as outlined in HIPAA guidelines if they are dissatisfied with the findings. The DCS Customer Relations Unit refers any questions to the DCS Privacy Officer.
7. If a complaint is sent to the *Federal Office of Civil Rights*, the Commissioner will be notified.

Note: State Attorney Generals may bring a civil action in federal court on behalf of state residents in any case in which the AG has reason to believe that an interest of one or more State residents has been or is threatened or adversely affected by any person who violates the HIPAA privacy and security rules, to enjoin the violation and for damages (up to $100 per violation, up to $25,000 per calendar year), and attorney fees.

Forms:

CS-0699, DCS Notice of Privacy Practices and Client Acknowledgment

Collateral Documents:

None