	DHS Head Start Program Policy		
PDM 18			
SUBJECT	Program Data - Access and Security		
REFERENCE	Program Design and Management		
EFFECTIVE	April 23, 2018		
Policy Council Approval: 1/22/19	**Policy Council Revision:** 5/23/23	**Governing Body Approval:** 2/28/19	**Governing Body Revision:** 6/15/23
			PAGE: 1 of 3

Policy:

The Head Start Grant Recipient and Education Service Providers must establish an internal procedure for proper access and security of program data for the City of San Antonio Department of Human Services Head Start and Early Head Program (DHS Head Start).

Procedure:

DHS Head Start utilizes ChildPlus as the secure database system for storing and tracking client information.

All user account holders are required to complete ChildPlus Access Request and ChildPlus User Security and Confidentiality Agreement forms. Upon completion, the forms are scanned and attached by the ChildPlus Administrator in ChildPlus under each respective user profile.

By accessing the database, staff understand and agree to abide by all terms of the ChildPlus User Security and Confidentiality Agreement and any applicable state and federal laws regarding Personally Identifiable Information (PII) and Protected Health Information (PHI).

- Education Service Providers are required to designate a staff member to complete the Personnel Profile for all staff members funded by the Head Start or EHS grant or anyone who works with children or families enrolled in the Head Start or EHS programs under the Management Module in ChildPlus. Designated staff is defined as preauthorized users in the Management/Personnel Module.
- Upon completion of the Personnel Profile, the designee will notify the ChildPlus Administrator if the user requires access to PII. Not all personnel require a ChildPlus user account.
- The ChildPlus Administrator will confirm with the designee the role of personnel and the types of access required.

- The ChildPlus Administrator will complete a User Security profile in ChildPlus, assign a login username and temporary password, restrict access by location, and designate User Security group(s).
- The ChildPlus Administrator will email the new account holder the login username and temporary password.
- The new account holder will log into ChildPlus and change the temporary password to a permanent password.

Authorized ChildPlus users are granted access under one of the following groupings:

- Staff: A ChildPlus personnel account will be created for all staff. ChildPlus user accounts and access is granted upon the approval of the ChildPlus Access Request Form and the completion of the ChildPlus User Security and Confidentiality Agreement Form.
- Education Service Providers: An assigned ChildPlus Super User for each Service Provider formally requests accounts via email for Service Provider Head Start Staff. Service providers are subject to the confidentiality provisions under the Family Educational Rights and Privacy Act (FERPA).
- Contracted Providers: A Special Projects Manager or designee will request user accounts for contractual providers via email or meeting with the ChildPlus Administrator. To meet the requirements of Health Insurance Portability and Accountability Act of 1996 (HIPAA), DHS Head Start requires any contract that include access to client information include an enforceable Business Associate Agreement (BAA). BAAs are documented in the professional services contract with the DHS Head Start.

Implementation of technical policies and procedures for electronic information systems that maintain electronic PII, PHI, and IDEA Part B and C to allow access only to those persons or software programs that have been granted access rights.

All DHS Head Start staff, regardless of position, share the responsibility to safeguard HIPAA, FERPA, PHI, PII, and the Individuals with Disabilities Education Act (IDEA) Part B and C data and information from unauthorized access, acquisition, or disclosure. Staff that share PHI, PII and IDEA Part B and C electronically must follow encryption guidelines and ensure the receiving entity is an authorized recipient of the specific data being delivered.

To ensure data protection, confidentiality, and to safeguard PHI, PII, and adhere to HIPAA, FERPA, and the Individuals with Disabilities Education Act (IDEA) Part B and C data, program staff should utilize a child or parent/guardian's ChildPlus ID and initials when communicating via email, TEAMS, or other electronic messaging system.

Staff may request parents/guardians to provide documents that contain PHI or PII via the secure ChildPlus Request Document feature.

Staff may utilize a program issued computer or device to access ChildPlus.

Staff ensures the environment in which they are working is secure and only authorized.

persons are within viewing distance of the authorized user's screen and/or confidential documents. Staff should use a privacy screen for all monitors and laptop screens as appropriate.

All devices (e.g., laptops and phones) must have auto-lock enabled with a maximum timeout of 15 minutes. Staff are encouraged to lock their workstations manually when leaving their desk (Windows key + L or CTRL+ALT+DEL).

Disclosure of ChildPlus information to a contractor is authorized but ONLY when an enforceable Business Associate Agreement (BAA) is in place.

All DHS Head Start staff must successfully complete the following trainings:

- COSA Security Awareness Training
- HIPAA Training

Completion of these trainings are documented and maintained by the City of San Antonio Human Resources Department and/or the Training and Technical Assistance Team.

All DHS Head Start staff must acknowledge the of CoSA Administrative Directives that include Data Security and Use of Technology.

Education Service Providers and contractors must develop and implement procedures to ensure all staff comply with this procedure and ensure all staff receive training on safeguarding FERPA, HIPAA, PHI, PII and (IDEA) Part B and C data.

Performance Standard:
1302.101(b)(4)