
		City of San Antonio Head Start Program Procedure			
		EFFECTIVE: April 23, 2018		REVISED: January 4, 2019	
SUBJECT: Program Data - Access and Security					
REFERENCE: HSPS 1302.101(b)(4)					
Policy Council Approval: 1/22/19		Policy Council Revision: 1/22/19		Governing Body Approval:	
				Governing Body Revision:	
PAGE: 1 of 2					

Purpose:

To 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 Start-Child Care Partnership (EHS-CCP) 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 understands and agrees 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-CCP grant or anyone who works with children or families enrolled in the Head Start or EHS-CCP 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 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 from unauthorized access, acquisition or disclosure. Staff that share PHI, PII and IDEA part B and C electronically must ensure the receiving entity is an authorized recipient of the specific data being delivered.

Only computers configured by ITSD for use on the CoSA network are authorized for accessing ChildPlus.

Staff may utilize a laptop and a secure means such as VPN, Workspace or Citrix 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.



Disclosure 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 annually:

- CoSA HIPAA 101 Privacy online training module
- CoSA HIPAA 102 Security online training module
- CoSA Employee Security Awareness Day in the Life online training module
- Completion of these trainings are documented and maintained by the City of San Antonio Human Resources Department.

All DHS Head Start staff must successfully review and acknowledge review and acceptance 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.

	City of San Antonio Head Start Program Procedure	
	EFFECTIVE: April 23, 2018	REVISED: January 4, 2019
SUBJECT: Management of Program Data		
REFERENCE: HSPS 1302.101(b)(4)		
PAGE: 1 of 2		

Purpose:

To establish an internal procedure for proper management of program data for the City of San Antonio Department of Human Services Head Start and Early Head Start-Child Care Partnership (EHS-CCP) Program (DHS Head Start).

Procedure:

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 FERPA, HIPAA, PHI, PII, and the Individuals with Disabilities Education Act (IDEA) part B and C data from unauthorized access, acquisition, or disclosure. Staff that share PHI, PII and IDEA part B and C electronically must ensure the receiving entity is an authorized recipient of the specific data being delivered.

- Only computers configured by ITSD for use on the CoSA network are authorized for the storage or transport of PHI, PII and/or IDEA part B and C data.
- Staff may utilize a laptop and a secure means such as VPN, Workspace or Citrix to access systems to view and maintain PHI, PII, and IDEA part B and C files.
- 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.
- Disclosure of PII and/or PHI, and/or IDEA part B and C to a contractor is authorized but ONLY when an enforceable Business Associate Agreement (BAA) is in place.
- Personal devices shall not be used to store or transmit unencrypted protected data.
- Any removable media or storage devices used to transfer PHI, PII, and/or IDEA part B and C data must be encrypted.
- If any PHI, PII, and/or IDEA part B and C data is transmitted via email attachment, the attachment must be protected by a password. The password to access the attachment must be sent to the recipient in a separate email.
- Hard copies (i.e., paper) of any PHI, PII, and/or IDEA part B and C data must be kept secured in a lockable file cabinet or other secured storage.
- In the event that PHI, PII, and/or IDEA part B and C data, either hard copy or electronic, are transported between locations, staff must take all precautions to ensure the materials remain secure and must remain in the presence of staff at all times.

Facsimiles

- Any documents received via facsimile, either telefax or online, that contain PHI, PII and/or IDEA part B and C data shall be uploaded or scanned into appropriate software (i.e., ChildPlus) as soon as possible. Any electronic copies of the facsimile should be saved to the user's desktop; once the upload is completed the file should be deleted and the deletion confirmed. Any hardcopies of the facsimile must be stored in a secure location or destroyed.
- Any hardcopies of the documents sent via facsimile, either telefax or online, that contain PHI, PII and/or IDEA part B and C data shall be either stored in a secure location or destroyed.

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

- CoSA HIPAA 101 Privacy online training module
- CoSA HIPAA 102 Security online training module
- CoSA Employee Security Awareness Day in the Life online training module

Completion of these trainings are documented and maintained by the City of San Antonio Human Resources Department.

All DHS Head Start staff must successfully review and acknowledge review and acceptance 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 receive training on safeguarding FERPA, HIPAA, PHI, PII and IDEA part B and C data.