	DHS Head Start Program Policy		
PDM 19			
SUBJECT	Management of Program Data		
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 2

Policy:

The Head Start Program, including the Head Start Grant Recipient and Education Service Providers, must 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 Program (DHS Head Start).

Procedure:

Implementation of technical policies and procedures for electronic information systems that maintain electronic Personal Identifiable Information (PII), Protected Health Information (PHI), and Individuals with Disabilities Education Act (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 Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act of 1996 (HIPAA), PHI, PII, and the IDEA Part B and C related data and information from unauthorized access, acquisition, or disclosure. Staff that share PHI, PII and IDEA Part B and C information electronically must ensure the receiving entity is an authorized recipient of the specific data being delivered.

- Only computers and or device configured by the IT Department for use on the CoSA network or Education Service Provider network are authorized for the storage or transport of PHI, PII and/or IDEA Part B and C data.
- Staff may utilize a program issued device 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. Staff should use a privacy screen for all monitors and laptop screens as appropriate.
- 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.
- 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).
- If any PHI, PII, and/or IDEA Part B and C data is transmitted via email, the email must be encrypted.
- 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.
- 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.
- Staff should not request PHI, PII, and/or IDEA Part B and C data via text or email. Staff may request parents/guardians to provide documents that contain this information via the secure ChildPlus Request Document feature.

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 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 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.

Performance Standard:
1302.101(b)(4)