

**HRSA DATA USE STATEMENT  
FOR THE  
HEALTHY START MONITORING AND EVALUATION DATA SYSTEM**

The purpose of this statement is to clarify how the Health Resources and Services Administration (HRSA) Maternal and Child Health Bureau (MCHB) intends to 1) use data for program monitoring and evaluation and 2) reassure that the data collected will be housed in a secure environment and 3) protect participant and program confidentiality.

**1. Purpose of Data Collection**

The Healthy Start Monitoring and Evaluation Data (HSMED) system allows MCHB to collect individual participant level data on all program participants from all Healthy Start programs. The data elements of the HSMED are populated using uniform data collection forms, the Healthy Start screening tools (OMB #: 0915-0338, Expiration Date: 11/30/2019). The HSMED also allows for internal analysis by MCHB to review data at both the national and grantee levels to determine impact and assess outcomes for Healthy Start participants.

**2. Security of Data**

The HSMED system is housed in a Fedramp-certified environment. Data are secured during transit through the Hypertext Transport Protocol (HTTP) on Secure Socket Layer (SSL) – HTTPS. Data storage is secured through 1) access control to ensure that data will be only accessed by authorized persons (designated by HRSA/MCHB staff) and 2) right level of access to ensure data integrity is maintained.

**3. Participant and Program Confidentiality**

All information provided by Healthy Start participants will only be used to monitor and evaluate Healthy Start programs. The only personally identifiable information (PII) required in the HSMED is date of birth (DOB) in order to link data and calculate age. This information, alone as the only PII, cannot identify participants.

For purposes of this statement, the data collected and provided to HRSA/MCHB are only to be used in aggregate statistical reporting. HRSA/MCHB will publish results of the evaluation in aggregate and any stratification (e.g. age, race/ethnicity, rural/urban, level of funding, etc.) will not allow the identification of individuals or grantees. No individual program data will be published to protect program confidentiality.