**Section 661.130 Data Submission**

a) The Registry shall be accessible to authorized users for the submission of information related to newborn blood spot, newborn hearing and newborn heart screening. Both demographic and newborn blood spot, newborn hearing and newborn heart screening data shall be reported by authorized users. Information shall include, but is not limited to:

1) Patient's name, date of birth, sex, telephone number, email address, home address, birthplace, and mother's legal name, as well as data concerning diagnosis, intervention, follow-up, parent support, parent-to-parent support and other outcomes for each child with a suspected or diagnosed condition through six years of age; and

2) Type of newborn screen, diagnosis, intervention, parent-to-parent support, parent support or follow-up administered, electronic health information such as Health Level 7 message, date of service, and identity of the provider who administered the newborn screen, diagnosis, intervention, parent support, parent-to-parent support or follow-up.

3) EHDI providers shall provide data to the EHDI Registry in accordance with Section 661.110.

b) An authorized user or the authorized user's designee shall submit newborn blood spot, newborn hearing and newborn heart screening, diagnosis, intervention, parent support, parent-to-parent support or follow-up data to the Registry in a manner defined by the Department.

c) Data may be provided electronically through the Department's web-based systems, through a secure integrated electronic system, or exchanged via Health Level 7 (HL7) 2.5.1 format or higher.

d) Authorized users shall provide an acceptable level of data quality, such as correct data fields, data accuracy, and adequate information to correctly identify or merge with existing records. Data shall be reviewed to determine data quality. Any rejected records shall be resolved by the user in no more than seven days. The Department will suspend system privileges and take any action, as appropriate, including termination for any user that submits inaccurate data or violates security policies.