Amendment to the *Homeless Management Information System (HMIS) Policies and Procedures Manual Ohio Balance of State Continuum of Care* in Response to the COVID-19 Pandemic

Ohio Balance of State Board Approval Date: March 23, 2020

Current Policy

IV. Security Standards, 3. Data Access Location

Policy: Users will ensure the confidentiality of client data, following all security policies in this document and adhering to the standards of ethical data use, regardless of the location of the connecting computer. All users are prohibited from accessing the HMIS database from any location other than the designated and approved work site.

Procedure: All Policies and Procedures and security standards will be enforced regardless of the location of the connecting computer. All HMIS related data entry will be processed at a designated and approved work site. A System Administrator will provide any additional clarification.

Amendment

Effective March 18, 2020 and until further notice, this amendment allows current HMIS users who need to access HMIS during the COVID-19 pandemic to do so while working remotely. This amendment does NOT change any of the other requirements for accessing HMIS, so any connection to HMIS regardless of data access location still must meet the other Security Standards listed in Section IV; particularly under sub-section A, items 5 and 6, with regard to Virus Protection and Firewalls.

Additionally a new policy and procedure is being added to address access from a Wireless (Wifi) internet source.

IV. Security Standards, 12. Wireless Access (Wifi)

Policy: A CHO and all authorized HMIS users must protect client level data, especially Personally Identifying Information (PII), while accessing HMIS from a device connected to the internet via a wireless network.

Procedure: Each Wireless or Wifi network that is being used to connect to the internet for the purpose of accessing HMIS must adhere to the following standards: a) the Wireless Network configuration must utilize a secure password to gain access or connect to the network or hot spot, and must use password encryption such as WEP, WPA or WPA2, b) the password must be stronger than the default password set by the network device.

Under no circumstances should an open or unsecured wireless network be used to connect to any network or the internet when accessing HMIS from the connected device.