MMIS ACCESS REQUIREMENTS

MMIS Access provisions are currently being updated to provide security enhancements which include alternative methods of authentication.

1. Contractor shall provide its own hardware, software and information technology support services necessary to meet the infrastructure requirements for accessing the Medicaid Management Information System (MMIS) production environment and/or other MMIS applications and/or the MMIS test environment as detailed below:

   A. Connection Options – Contractor shall use one of the following:
      i. Leased line from Contractor to OHCA's fiscal agent with an Ethernet or Fast Ethernet handoff; or
      ii. VPN (virtual private network) connection across the internet to OHCA's fiscal agent with high speed internet access and as well as a device capable of establishing a VPN tunnel with OHCA's fiscal agent's hardware; or
      iii. Internet Browser compatible with OHCA version (currently utilizing: Internet Explorer Version 7.0 or above).

   B. Transmission – Contractor shall encrypt all connections with OHCA's fiscal agent utilizing all of the following minimum standards:
      i. Authentication Algorithm- SHA;
      ii. Encryption Algorithm- AES 256;
      iii. Group 5 Diffie-Hellman; and
      iv. Security Protocol- ESP

   C. Authentication - Contractor shall establish a one-way Microsoft Active Directory trust with OHCA's fiscal agent in which the fiscal agent will trust the Contractor with one of the following to ensure that Domain controllers and DNS (domain name system) servers on both networks communicate properly:

      Either servers with publicly registered IP (internet protocol) addresses or servers with private IP addresses which require the following:

      i. Static NAT (network address translation) for each Domain Controller and DNS server (IP range to be assigned by OHCA's fiscal agent).
      ii. A manually configured DNS Zone with all DNS servers and Domain controllers only on the Contractor's network. This zone shall be manually set to reflect the Static NAT addresses of each of the servers.

   D. Once an acceptable DNS Zone is established for the trust, OHCA's fiscal agent and the Contractor shall exchange DNS records. Contractor shall update and exchange DNS records if additional Domain Controllers are added to the Contractor's network.

2. Contractor shall:

   A. Submit requests for employee passwords for the MMIS;
   B. Train appropriate staff to use the MMIS;
   C. Notify OHCA when an issued password is no longer needed due to termination of employment or change in duties within five (5) business days;
   D. Ensure that its employees are informed of importance of system security and confidentiality including HIPAA;
   E. Document and notify OHCA of system problems to include type of problem, action(s) taken by Contractor to resolve problem and length of system down-time within eight (8) hours of problem identification; and
   F. Provide a Microsoft Active Directory user account for use with the MMIS production environment.