

## **MMIS CONNECTIVITY REQUIREMENTS**

The Contractor shall provide its own hardware, software and information technology support services as shown below as necessary in conformance with the following requirements:

- a. Use an Internet Explorer version acceptable to OHCA;
- b. Connection Options – Connect to OHCA’s MMIS using non-RFC (Request for Comments)1918 addresses with one of the following:
  1. Leased line from Partner to OHCA’s fiscal agent with an Ethernet, Fast Ethernet, or Gigabit handoff;
  2. Dark fiber or dark copper connection with an Ethernet, Fast Ethernet, or Gigabit handoff; or
  3. Establish a VPN (virtual private network) connection across the internet to OHCA’s fiscal agent using a high speed internet service and a device compatible with OHCA’s fiscal agent’s hardware.
- c. Transmission –Encrypt via IPsec (Internet Protocol Security) all connections with OHCA’s fiscal agent utilizing all of the following minimum standards:
  1. Authentication Algorithm – SHA (Secure Hash Algorithm);
  2. Encryption Algorithm – AES (Advanced Encryption Standard) 256;
  3. Group 5 Diffie-Hellman; and
  4. Security Protocol – ESP (Encapsulating Security Payload)
- d. Authentication –Establish a Federated Trust with the existing Microsoft Active Directory Federation Service (ADFS) and meet the following requirements:
  1. Compatible with Microsoft Windows 2008 R2 ADFS
  2. Enable JavaScript and cookie policies for browser-based sign-in and sign-out.
  3. Obtain three certificates for ADFS setup:
    - Service communication certificate – This is a standard SSL (secure sockets layer) certificate that is used for securing communications between federation servers and clients;
    - Token-Signing Certificate – This is a standard X509 certificate that is used for securely signing all tokens that the federation server issues; and
    - Token-Decrypting certificate – This is a standard SSL certificate that is used to decrypt any incoming tokens that are encrypted by a partner federation server;
  4. Configure and maintain Active Directory Groups to address application authorization;
  5. Configure organization custom claims for MMIS Applications.

## **MMIS SFTP (SECURE FILE TRANSFER PROTOCOLS)**

The Contractor shall provide its own hardware, software and information technology support services as shown below as necessary in conformance with the following requirements:

- a. A secure ftp application which supports public keys
- b. A firewall which supports the following
  1. Public IP address
  2. NAT subnet (if applicable)
- c. Contractor operating systems

1. Compatible with unix
  2. Compatible with Microsoft Windows
- d. Application specifics
1. Establish an account name for the directory/folder for data reception/origination
  2. The account name will be used in lieu of a password
  3. OHCA's fiscal agent's sftp platform will initiate the connection to the Contractor platform using the Contractor account name and IP address
- e. Connection Options – Connect to OHCA's Medicaid Management Information System (MMIS) using non-RFC (Request for Comments)1918 addresses with one of the following:
4. Public internet (peer to peer)
  5. Establish a VPN (virtual private network) connection across the internet to OHCA's fiscal agent using a high speed internet service and a device compatible with OHCA's fiscal agent's hardware.
- f. Transmission –Encrypt via IPSec (Internet Protocol Security) all connections with OHCA's fiscal agent utilizing all of the following minimum standards:
5. Authentication Algorithm – SHA (Secure Hash Algorithm);
  6. Encryption Algorithm – AES (Advanced Encryption Standard) 256;
  7. Group 5 Diffie-Hellman; and
  8. Security Protocol – ESP (Encapsulating Security Payload)