TEXAS Health and Human Services | Texas Department of State Health Services

Texas Immunization Registry

Secure File Transfer Protocol Specifications

Background

The Texas Immunization Registry offers secure File Transfer Protocol (FTP) as a data exchange method for health care entities required to report patient and immunization data to the registry as indicated by state law. The registry supports the ImmTrac2 application.

Purpose

The Secure FTP Specifications are to be used by all organizations submitting patient and immunization data to the registry via unidirectional data exchange.

Secure FTP Methods

The registry supports the following three methods, listed in order of preference.

Organizations and their electronic health records (EHR) vendors should not connect to SFTP using an IP Address but via one of the three described methods.

HTTPS

- View, upload and download files securely with Secure Sockets Layer (SSL) encryption on a standard internet browser.
- **Host Name: https://immtrac-ftps1.dshs.state.tx.us/ThinClient**
- Encryption Settings: Use your browser's default security settings
  - Google Chrome is the recommended web browser for use.
- Port Information (should be open on your network fire wall): Port 443 (standard HTTPS port)

FTPS

- Requires secure FTP client software to upload/download files securely using Implicit SSL/Transport Layer Security (TLS) version 1.2 encryption or higher.
- **Host Name: immtrac-ftps1.dshs.state.tx.us**
- Encryption Settings: Requires at least 128-bit encryption for secure connections:

  - SSL Type = Implicit SSL
  - SSL Security Level = TLS Only
- Port Information (should be open on your network fire wall): Remote Port = 990 FTPS
- NOTE: If using FTPS with passive mode, which is not commonly used, the following Port Information must be used: Remote Port = 990 (handshake) Communication Ports = 5000 through 5010 (data)
- Recommended Settings:
  - Verify Deletions - Enabled
  - Connection Retries - 0 (zero)
  - Connection Retry Delay - 30 (seconds)
  - Network Time out - 65 (seconds)
  - Keep Alive - 0 (zero)
    - Do not leave FTP connections alive for more than necessary.
    - Once the file transfer(s) have completed, configure your FTP client software to disconnect.
- Encryption Information: No client certificate is needed for your FTPS client, but you may see a Trusted or Non-Trusted Certificate window which asks if you choose to accept the registry's server certificate. The security certificate is safe to allow/trust on your computer. The options are:
  - Select "Trust this certificate" (recommended) if you select this option, your FTP client software will not show you this message again.
  - Select "Allow this connection only" and you will be allowed access and prompted each time for future connection attempts.
  - Selecting "Do not allow this connection" will not allow you to connect during this session and you will be prompted again to accept the FTP server certificate for future connection attempts.

NOTE: Your network support team may have to configure your LAN firewall and NAT to allow FTP connections if your FTP client software resides on a machine that has a private IP address.

SFTP

- Requires secure FTP client software to view, upload or download files securely using Secure Shell (SSH) encryption.
- **Host Name: immtrac-ftps1.dshs.state.tx.us**

- Encryption Settings: Server/Connection Type SFTP/SSH
- Port Information (should be open on your network fire wall): Remote Port = 22
- Recommended Settings:
    - Verify Deletions - Enabled
    - Connection Retries - 0 (zero)
    - Connection Retry Delay - 30 (seconds)
    - Network Time out - 65 (seconds)
    - Keep Alive - 0 (zero)
        - Do not leave FTP connections alive for more than necessary.
        - Once the file transfer(s) have completed, configure your FTP client software to disconnect.
- Encryption Information: Public keys can be e-mailed via encrypted e-mail to the registry's Interoperability Team after an organization has completed their registration of intent.
    - Use of a FTP server default public key may be used in which the password will be required on every login.
    - If configuring SFTP with no password, SFTP users may still be required to use the assigned default password on the initial connection.
    - For SFTP public keys created on a Unix/Linux machine and your organization has provided the registry with the public key but you are still being required to type in the password, please contact the registry's Interoperability Team for assistance.
    - The Interoperability Team will inform you when to start sending test or production data from the organization.

Scripting User Folder Paths

The import code is assigned by the registry and provided to the organization at the time the FTP account is created. The import code is also the FTP username and root folder name.

<u>Important Information:</u>
Once logged into the FTP user account, mostusers will default to their respective root folder.

To upload and copy files using scripts, the FTP client should be written to navigate to the subfolders. Users only have list privileges (rights) on the root folder.

Below are the subfolders using the short paths and respective subfolder privileges (rights).

***/[importcode]/*Accepted** - contains the original HL7 files submitted.

- List and read rights.

***/[importcode]/*DQA-Report** - contains the data quality assurance (DQA) reports for all the HL7 files processed.

- List and read rights.

***/[importcode]/*HL7-Dropoff** - used to place all inbound HL7 files for processing.

- List, read, write, rename, and delete rights.

***/[importcode]/*Receive** - contains all consent notification files (CNF) received after the HL7 files are imported.

- List and read rights.

For more scripting tips, please refer to your FTP client software support site.

Interface Configuration

Once connected to the registry's FTP server, the basic FTP client interface looks like Figure 1 – FTP Interface.

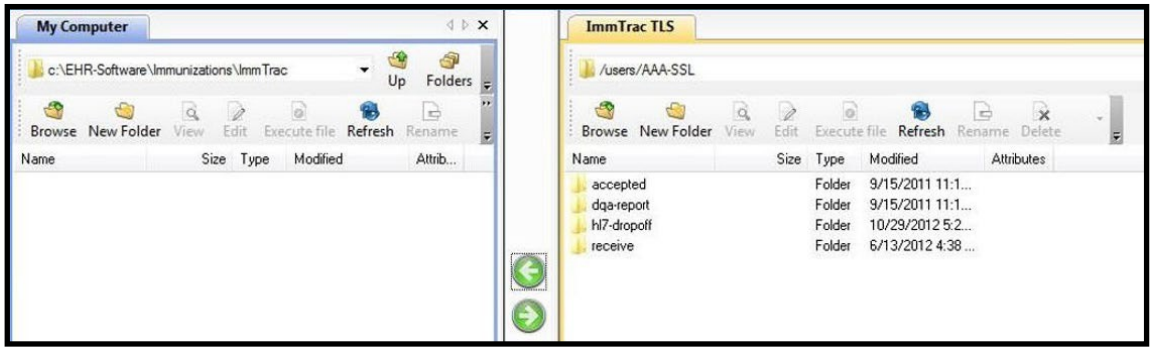

Figure 1: FTP Interface

The left side of Figure 1 shows "My Computer" as your workstation (server). The right side of Figure 1 shows the "ImmTrac TLS" as the registry's secure FTPS server with an example FTP user account of AAA-SSL.

FTP User Responsibilities and Reminders

- Communicate and coordinate with your organization's IT desktop support, EHR and/or network staff to resolve connection issues.
- If the FTP client connection attempts do not show up on the registry FTP logs, it's likely a connection issue on the FTP client end.
- Change your password during initial login.
- The registry does not store FTP passwords for retrieval and can only reset passwords.
    - Request to reset the FTP password must be made by the point of contact indicated in ImmTrac2 for the health care entity.
- The registry's FTP Server does enforce a file quota limit of 300 files for user folders.

Texas Immunization Registry Actions

The registry purges data older than 180 days and reserves the right to update its security keys as needed. Registry staff are not authorized to provide support for network issues you may be experiencing on your computer or network and FTP software client issues.

Contact Information

For more information and support contact the Texas Immunization Registry Interoperability Team.

Email: ImmTracMU@dshs.texas.gov

Phone: (800) 348-9158, press Option 3