Purpose of WTC Guide
The ImmTrac Secure Web Transfer Client (WTC) Guide is written to help providers maintain security and quality of client data throughout the reporting process to and from ImmTrac the Texas Immunization Registry. WTC uses standard HTTPS with SSL to safely view and transfer data securely to and from ImmTrac – The Texas Immunization Registry. The WTC allows users access to their FTP folders using a standard internet web browser for viewing and transferring files securely. If your site automates your FTP connectivity and/or file uploads/downloads, there are secure FTP 3rd party software available on the internet. If your site needs more information on what is allowed and available on your provider’s network and computers, please ask your site’s information technology (IT) team and/or EHR software vendor about secure FTP automation. Be advised the ImmTrac WTC does not use the same login as the ImmTrac Web Application. Once the provider has been issued FTP login credentials, the authorized FTP user(s) are only accessing that registered provider’s electronic data folders.

Immunization Providers, EHR Software Vendors and ImmTrac FTP Responsibilities
Most providers reporting immunization data to ImmTrac use EHR (Electronic Health Record) software in their practices. While the terms “EMR” and “EHR” are often used interchangeably, EMR solutions allow for patient information to be shared within one health care organization, whereas EHR solutions allow for health-related records to be shared across multiple organizations. Each provider may be setup differently in regards to their local network, EHR/EMR’s and client databases. ImmTrac – The Texas Immunization Registry cannot recommend 3rd party FTP software to providers and/or EHR Vendors. It is the responsibility of the provider to determine whether or not data reporting to the Texas Immunization Registry will be automated or a manual process on the provider’s side. It is also the responsibility of the registered ImmTrac provider to work with their EHR vendor to determine if their current EHR and EHR Vendor Services supports secure FTP data transfers.

FTP Security Responsibilities
Before continuing with this guideline for the ImmTrac WTC, it is important to know a few security responsibilities about reporting data to and from ImmTrac. Most importantly, access to the ImmTrac Secure FTP server is the main responsibility of the ImmTrac registered provider. Secondly, each registered site/provider is only issued one set of secure FTP login credentials. FTP credentials are considered “Service Accounts”. Service account passwords do not expire and are not required to be changed. ImmTrac highly recommends that ImmTrac registered providers work with their IT department and/or their EHR software vendor to coordinate password changes and responsibility of securing and maintaining the provider’s FTP account.
If and when a person with FTP access information either from a third party (e.g. EHR vendor) or internal provider staff member is no longer employed or duties have changed, please coordinate with the EHR software and/or IT department to change the FTP password. Although ImmTrac can work directly with EHR software vendors in helping providers connect to the ImmTrac FTP server, it is the responsibility of the provider to maintain control of the ImmTrac FTP WTC account. ImmTrac will not provide technical and/or account support to provider staff and/or EHR software vendor personnel unless the listed ImmTrac main point of contact at the provider site has given ImmTrac written (via e-mail) authorization for that specific individual. A provider main point of contact can list more than one FTP contact if necessary.

Any updates for adding or dropping person(s) from the list of authorized users should be e-mailed to immtrac@dshs.state.tx.us. For all FTP support related inquiries, please type in “FTP Support” in the subject line and include your full name/e-mail signature, Import Code and screenshots of any error messages you are encountering.

It is also important to note that because providers switch EHR vendors from time to time, the method of how client data is exchanged can also change. ImmTrac offers a few industry standard secure FTP methods to report data. The ImmTrac WTC is a “manual upload” secure FTP connectivity option. ImmTrac also allows SFTP (with SSH) and FTPS (with SSL) for connectivity to ImmTrac’s secure FTP server and each of these methods can be automated or used for manual uploads. Again, FTP configuration setups on the providers end are solely the responsibility of the provider when deciding which method to use. It is extremely important that providers communicate with their EHR software vendors on which method they will use and it is the also the responsibility of the provider to ensure that whichever method is chosen, the login credentials and/or if applicable, any private/public keys pairs are also stored and used securely by the EHR.
Logon

Go to https://immtrac-fts1.dshs.texas.gov/ThinClient/Login.aspx and logon using your ImmTrac FTP secure credentials.

If you see the security box open at the bottom of your screen (as shown below), please click on the drop down next to “No” and choosing “Don’t Ask Again”. Choosing “Yes” is not recommended for shared computer user profiles.
Home Page
You will arrive at the “Home” page/screen below.
Change Password
You will find the “Change Password” option on the upper right portion of your Home screen. Click on this link.
The password change dialogue box should now be opened. You may now change your password. It is required that your password:

- Has at least eight characters
- Includes at least two numbers
- Has at least one special character.

Please also note:

- The ImmTrac FTP login ID is not the same as the ImmTrac web application login ID that allows providers to directly search and edit immunization records for all Texas clients in the Texas Immunization Registry database.
- It is highly recommended when a provider has an EHR vendor that uploads their client data, the providers request that their EHR software vendor also retrieve the provider’s “return/notification files” which may include “Data Quality Analysis (DQA) Reports” with providers submitting and receiving in HL7 data format.
- If providers have an EHR vendor that submits client data for a provider, the provider should coordinate with the EHR when there is a password change. This is especially important when data transfers are automated by the EHR on behalf of the provider.
- Passwords do not expire, but it is highly recommended that the provider change it at least yearly.
- You do not have to change password on the initial login.
Once you have filled in all password fields correctly, Click “OK”.
Once you click “OK”, you will be returned to the Home page where you will see the message that you have successfully changed your password.
FAQ
The Frequently Asked Questions (FAQ) link is to the right of “Change Password” Link.

[Image of FTP client interface]
(FAQ – continued)

Once you have opened the FAQ web page, note that you also have the ability to **Print** this page (upper right corner of the screen) for easy reference. Once you are done, you may close the tab to exit.
Folders
As noted you will find your folders on the main page. The “Submit” is where you may upload your files for processing. The “Receive” folder will contain all ImmTrac Notification Files received after ImmTrac validation/importation.
Uploading Files
At the top of the screen, please note the tab locations for UPLOADING FILES. You will not be able to upload on the Home screen. The only folder you will have rights to upload data in is the “Submit” folder. Click on the “Submit” folder. In order to provide a better understanding, we will walk you through the process of uploading files.
(Uploading Files – continued)

In the “Current Folder” file you will notice the “/Submit” folder is indicated. Next, click on the “Upload Files” tab.

The UPLOAD FILES window will then pop up. You may then browse your computer resources to locate the file you wish to upload and click on “UPLOAD” to submit.
In the event that you need to overwrite the file you’re sending (possibly if you’re sending us a replacement or corrected file, or taking some similar action), you’re given the opportunity on the UPLOAD FILES pop up window. You may check the box “Overwrite selected Files on the server” and then click “UPLOAD”. Once you click on “UPLOAD”, whether or not you’ve checked to Overwrite, you will be returned to the main screen where you will find confirmation of the Upload success or failure.
1. On the next screen you should see the message that your file has been successfully uploaded.
2. You should now see your file in the “Submit” folder.
3. To get back to the Home screen, click on the “Home” tab.
**Downloading/Copying Files**

On the Home screen click on **“Receive”**
The “Current Folder” should indicate that you are in the “\Receive” folder. Click the check box next to the file you want to download and then click on the “DOWNLOAD FILES” tab.

A window, similar to the one below, will pop up on the screen. Click on “Save” and choose which save option you prefer. A Windows Explorer box will open and you will be able to save the file to your computer.

A pop-up window similar to the one below will confirm your file was saved.
Logging Out
To log out of the ImmTrac WTC website click on “Logout” in the upper right hand corner of your screen.

File Processing
Please allow three to seven business days for processing. Once your file has been processed, you will be able to review the return file in the “Receive” folder. In the “Receive” folder, you may view the file or you may select the file (by checking the box to the left of the file name) and then click on the “DOWNLOAD FILES” tab to retain a copy for your records. Be advised that because ImmTrac cannot regenerate return files, deleting files in this folder is not allowed. Your return files will be held for 90 days. After 90 days notification/return files will be purged.