Texas APCD Technical Guide

Version 1.0

October 05, 2022

The University of Texas
Health Science Center at Houston

School of Public Health

Center for Health Care Data

Contents

1.0. Document Version History 5
2.0. Introduction and Overview 6
2.1. The Center for Health Care Data at UTHealth Houston 6
2.2. Texas Advanced Computing Center (TACC) 6
2.3. Complementary Documentation 7
2.4. Technical Guide 7
2.5. Flow Overview 8
Figure 1: Submission Flow 8
Figure 2: Validation Process 10
3.0. Obtaining a TACC TX-APCD User Account 12
3.1. Steps to Obtain User Account 12
4.0. Registration 13
4.1. Online Registration 13
4.2. Offline Registration 13
4.3. Registration Notes 13
4.4. Submitter Identifiers 14
4.5. Submitter Encryption Key 15
5.0. Preparing Files for Submission 16
5.1. File Naming Requirements (with example) 16
Figure 3: File Naming Rules 16
5.2. General Data File Format (with example) 16
5.3. Preparing the File Package 17
5.3.1. Obtaining the 7-Zip Tool 17
5.3.2. Installing the 7-Zip Tool 18

5.3.3. Creating a Zip File Package 18
5.3.4. Splitting a Zip File Package 24
6.0. Submitting Data to the TX-APCD 27
6.1. Setting Up Multi-Factor Authentication on Your TX-APCD User Account 27
6.2. Secure File Transfer 29
6.2.1. Command Line Methods 29
6.2.2. Graphical User Interface Methods 30
6.2.3. Confirming File Transfer Success 34
6.3. Secure Web Transfer (HTTPS) 35
6.3.1. Login to the Submitter Portal 35
6.3.2. Upload a File Package 35
6.3.3. Confirming Receipt of Transfer 38
6.4. Encrypted USB Disk 38
6.4.1. Selecting a Secure USB Drive 38
6.4.2. Preparing the Data File(s) 38
6.4.3. Selecting a Courier 39
6.4.4. Sending the Package 39
6.4.5. Data Transfer to the TX-APCD 40
6.4.6. Confirming Receipt of Transfer 40
7.0. Submission Testing 41
7.1. Submission Definition 41
7.2. Processing of Data Submissions 41
7.2.1. Stage 1 41
7.2.2. Stage 2 42
7.2.3. Stage 3 42

7.3. Identification of Test Submissions 42
7.4. Test Guidelines 42
7.4.1. Current Information 42
7.4.2. Purpose 43
7.4.3. Size 43
7.4.4. Frequency 43
7.4.5. Success 43
APPENDIX A – Abbreviations/Acronyms Used 45

1.0. Document Version History

VERSION HISTORY		
Version Number	**Date Published**	**Summary of Revision**
0.01	08/15/2022	Initial draft for review following the publication of notices related to registration and testing.
1.0	10/05/2022	First published edition.

2.0. Introduction and Overview

The 87th Texas Legislature enacted House Bill 2090, which became effective on September 1, 2021, and provides for the creation of a Texas All-Payor Claims Database (TX-APCD) to be developed and administered within The University of Texas Health Science Center at Houston (UTHealth Houston) and UTHealth School of Public Health (SPH) Center for Health Care Data (CHCD). The database is designed to increase transparency of health care information to the public and improve the quality of health care in the state of Texas.

The rule adopted by the Texas Department of Insurance (TDI) at 28 Texas Administrative Code §§21.5401–5406, concerning the TX-APCD, identifies compliance requirements for submitters. The regulations are directly related to the details within this technical guide.

2.1. The Center for Health Care Data at UTHealth Houston

The CHCD at UTHealth Houston is a Centers for Medicare and Medicaid Services (CMS) Certified Qualified Entity (QE) with proven expertise in the collection, management, and analysis of administrative claims data and adjacent health care data. The CHCD has been certified by CMS as meeting its rigorous requirements for data privacy and security. The CHCD is a non-profit entity, operating within UTHealth SPH. It is independent from all provider organizations and health plans and maintains a mission of data informing policy and driving value in health care outcomes. For more information on the TX-APCD or the UTHealth Houston CHCD, visit the following website at https://go.uth.edu/txapcd.

2.2. Texas Advanced Computing Center (TACC)

The Texas Advanced Computing Center (TACC) is a division of the University of Texas at Austin located on the J.J. Pickle Research Campus in Austin, Texas. TACC has been in operation for over 20 years, provisioning compute infrastructure and expert staff to support and execute thousands of high performance computing (HPC) data-driven projects over the years. In the role of datacenter partner for the TX-APCD, TACC will provide datacenter and related services to host all TX-APCD data, along with providing the infrastructure and software tools necessary to process and analyze and report on the data.

2.3. Complementary Documentation

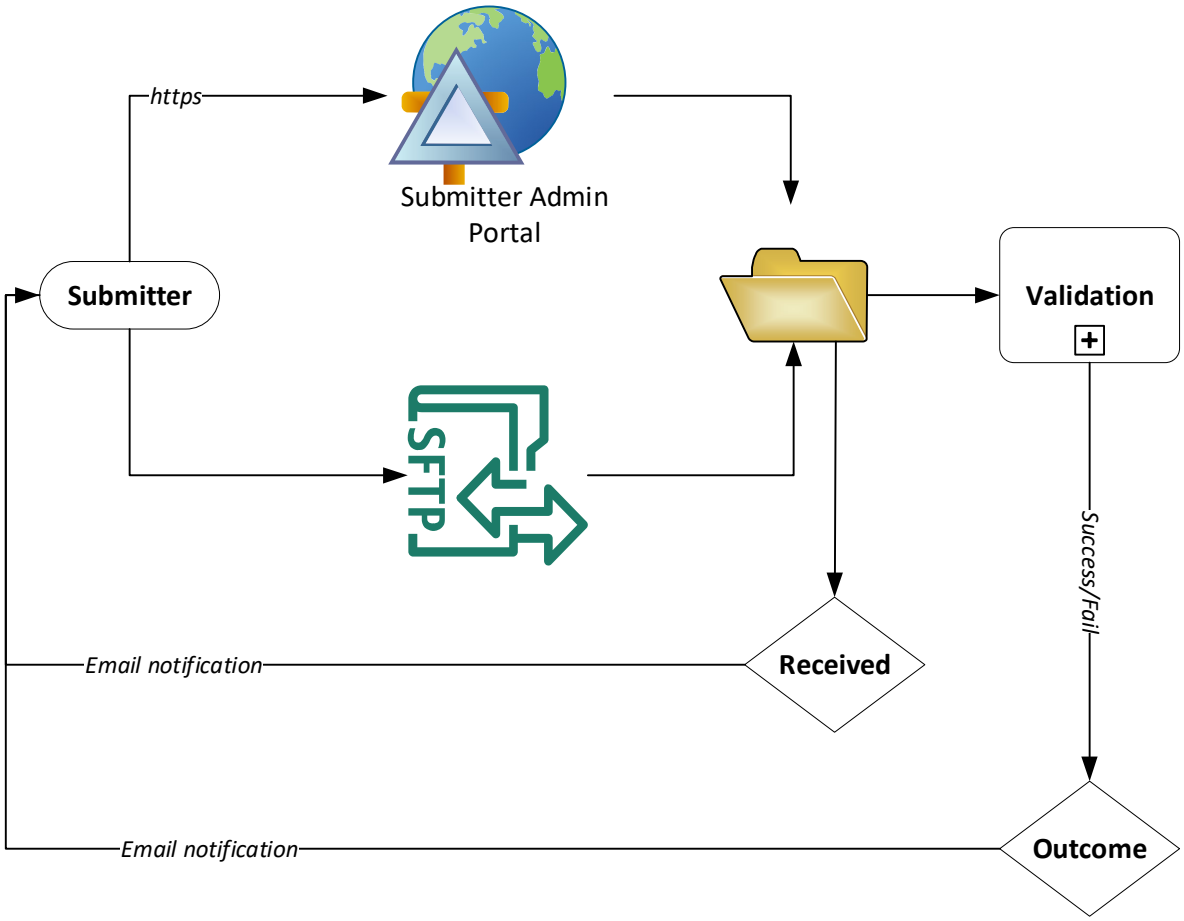
Before working with this technical guide, please be sure to download and review both the Data Submission Guide (DSG), and the Common Data Layout (CDL). These documents lay the foundation for this technical guide and the three documents are intended to be used together.

2.4. Technical Guide

This technical guide is intended to address the technical aspects of connecting users to TACC computing resources and submitting data to the TX-APCD. Topics to be covered include (a) how to obtain a TX-APCD user account, (b) how to register your organization with the TX-APCD, (c) how to obtain a submitter identity and encryption key, (d) how to create and prepare data file packages for submission, (e) how to submit data file packages using one of the three submission methods, (f) samples of what the data files should look like, (g) how to subscribe to system notifications, and (h) if necessary, how to resubmit a file package to correct errors from a previous submission.

2.5. Flow Overview

Figure 1: Submission Flow



Submitters have the option to submit files via secure file transfer protocol (SFTP) or hypertext transfer protocol secure (HTTPS). Both options will be discussed in detail in this technical guide. A third method, using an encrypted universal serial bus (USB) drive, will also be described in detail.

When a file package is successfully transmitted to the TX-APCD, the submitter will receive an email confirmation indicating that the package has been received. Once the submitted files have been received, the files will be validated. The submitter will be notified by email with information containing details about the outcome. Submitters can subscribe to these notifications when registering by selecting the checkbox to receive system notifications on the registration form.

Figure 2: Validation Process

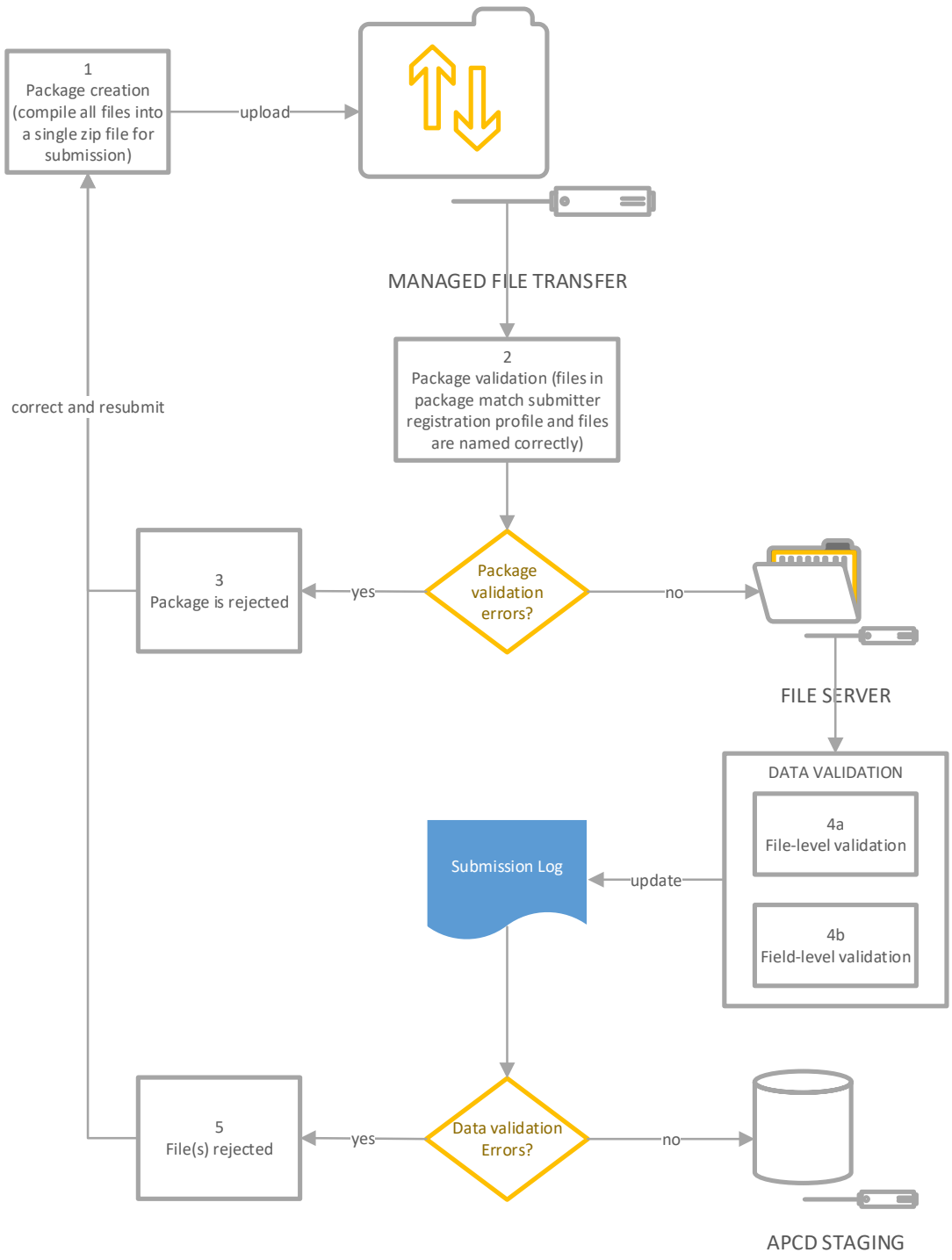


Figure 2 describes the validation process. A successful file validation process only indicates that the file contents are consistent with the rules specified in the CDL. Subsequent checks will be performed to ensure that the data is logically consistent.

3.0. Obtaining a TACC TX-APCD User Account

Before being able to interact with the TX-APCD, a TACC user account is required to access computing resources. A user account can be requested by going to https://accounts.tacc.utexas.edu/apcd/register, providing the requested information, and then submitting the request. The request will be reviewed, and a confirmation email will be sent to the user with guidance on how to use the account to interact with the TX-APCD.

3.1. Steps to Obtain User Account

1. Open a browser (Chrome/Edge/Firefox – Chrome is preferred) and navigate to https://accounts.tacc.utexas.edu/apcd/register.
2. Read the instructions provided before continuing.
3. Fill out the form as accurately as possible. It is important to use a business email when requesting a user account. As you type your organization name, it will be matched with a database of known organizations. If no match for your organization name is found, be sure to type in the complete and official name of the organization you belong to. New organization identities must be approved by administrators prior to approving a new account request which may incur an additional two business day delay in the account approval process.
4. Submit the form by clicking on the "Create TACC Account" button.
5. Check the mailbox for the email you specified in the request. You should receive an email titled "TACC Account Action Required: AUP confirmation" containing a link to TACC's Acceptable Use Policy (AUP). Click the link to view the AUP.
6. The AUP details your legal obligations while using TACC resources. Please scroll and read the AUP in its entirety, check the "I agree to the terms of the TACC Acceptable Use Policy" and click on the "SUBMIT" button.
7. Your account will be reviewed, and you should receive a response to your account request within two business days.

4.0. Registration

Once your TACC account is approved, the next step in the process is to make sure your organization is registered with the TX-APCD (if not already registered). Organizations must be registered before being able to conduct any transactions (data submission) or submit any requests (i.e. extensions or exceptions) to the TX-APCD. Any requests for submission exceptions and/or extensions can only be addressed for organizations which are registered.

4.1. Online Registration

Note: This section is under development and will be published in a future version release of the Technical Guide.

4.2. Offline Registration

An organization can register for the TX-APCD by using the portable document format (PDF) registration form which can be downloaded from the website at https://go.uth.edu/txapcd under the "Entity Registration" section. Complete the form and submit to the email provided in the instructions on the website. Please provide accurate contact information in the form as you may be contacted by the TX-APCD operations team for clarification or additional guidance.

4.3. Registration Notes

All carriers that do business in Texas will need to register with the TX-APCD; there are no small plan exceptions. Eligibility for exceptions and/or extensions cannot be determined until registration is successfully processed. The same applies for plan administrators (third party administrator [TPA]/administrative services only [ASO]) who may be submitting data on behalf of any health plans within the scope of the law.

On the Registration Form, all sections should be completed unless stated otherwise (for instance, where it states "fill in all that apply"). The Claims Estimates section of the Registration Form is inclusive of all claims (e.g., medical, pharmacy, dental) as of December 31 of the previous year and should be filled out accordingly.

An organization is required to submit a single registration during the initial registration period (October 10, 2022 – November 10, 2022), and a registration renewal each year thereafter. Any

subsidiaries or business units of the organization which are in scope of the TX-APCD rule should be identified in the Entity section of the registration form. Identifiers will be assigned both to the organization and to each submitting entity.

To ensure the appropriate contacts receive system notifications (under Contact Information), click the box “select to receive system notifications” for those listed to get email notifications about the processing of data submissions. It is important to note that emails sent from the TX-APCD will be sent from one of the following domains:

a. txapcd.org

b. uth.tmc.edu

c. tacc.utexas.edu

In order to avoid emails sent to you being rejected, placed in quarantine, or sent to your junk folder, the domains listed above should be configured as “safe senders” in your email client. Please consult your system administrator for assistance with this.

Note: System email notifications may include attachments which could be of type zip, html, pdf, json, csv, or xlsx.

The key outcome of the registration process is the assignation of a submitter code, payor code(s), and encryption key(s). These three pieces of information are critical for creating and preparing data files for submission. They will be assigned by the TX-APCD operations team to each submitter. A submitter is an identifiable entity that submits data to the TX-APCD. It could be a standalone company, or a subsidiary, or business unit of a company group or umbrella organization. It is important to handle this information with care. In the event that you believe your encryption key has been compromised in any way, please request a replacement as soon as possible.

4.4. Submitter Identifiers

In this guide, the term “submitter” will be used to represent an entity (a company or subsidiary of a company) which submits data to the TX-APCD. After a determination has been made that the registering organization is required to submit data under the regulations, the next step is

determining whether one or more "submitters" should be created for the organization. If a single organization has multiple submitters and the organization has multiple subsidiaries/units doing business in the state, then each subsidiary/unit qualifies as a submitter. However, there could be other reasons why multiple submitters might be established for a single organization. This determination will be made by the TX-APCD operations team in consultation with the registering organization.

Two identifiers will be assigned by the TX-APCD to each submitter (each entity that will submit data).

1. Submitter Code – this is an alphanumeric code that identifies the overall submitter and can be no more than 8 characters in length. It will be in the form of a mnemonic of the organization's name. For example, TWOSTEP might be assigned as a submitter code for Two Step Health Insurance Company.
2. Payor Code – this is an 8-digit code that identifies the company, subsidiary, business unit or plan for which data is being submitted. For example, TWOSTEP might be assigned the Payor Code 87202335 at the discretion of the TX-APCD operations team.

It is important to note that these two codes are elements CDLXX001 and CDLXX002 in all data files described in the CDL, both of which are mandatory (even though the Payor Code is listed as "optional" in the CDL).

4.5. Submitter Encryption Key

Data files submitted to the TX-APCD must be zipped and encrypted. As part of the registration process, each submitter is assigned a unique encryption key that must be used to encrypt the data file package before it is submitted to the TX-APCD. The encryption key ensures that the data file package is not tampered with before or during the submission process. The TX-APCD reserves the right to assign a new encryption key to a submitter periodically, with at least 45 days of notice before the new key is required for new submissions. A submitter can also request a new encryption key in the event that the assigned key has been compromised.

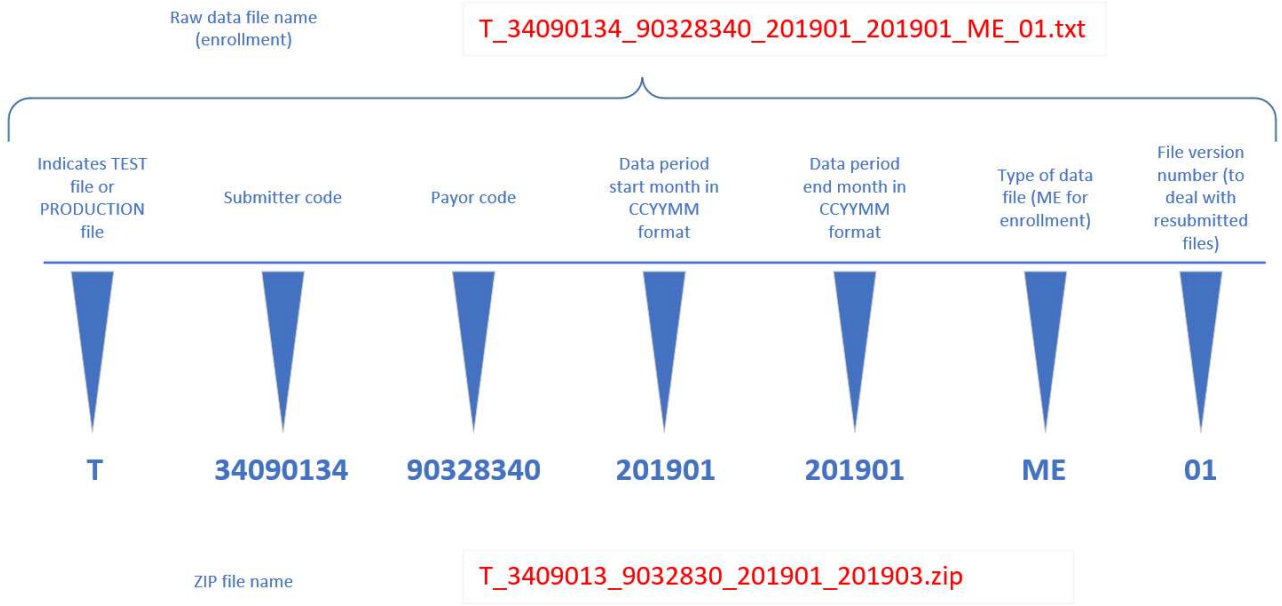
5.0. Preparing Files for Submission

After successfully registering and obtaining the identifiers and encryption key required for the process to work, files can be prepared for submission.

5.1. File Naming Requirements (with example)

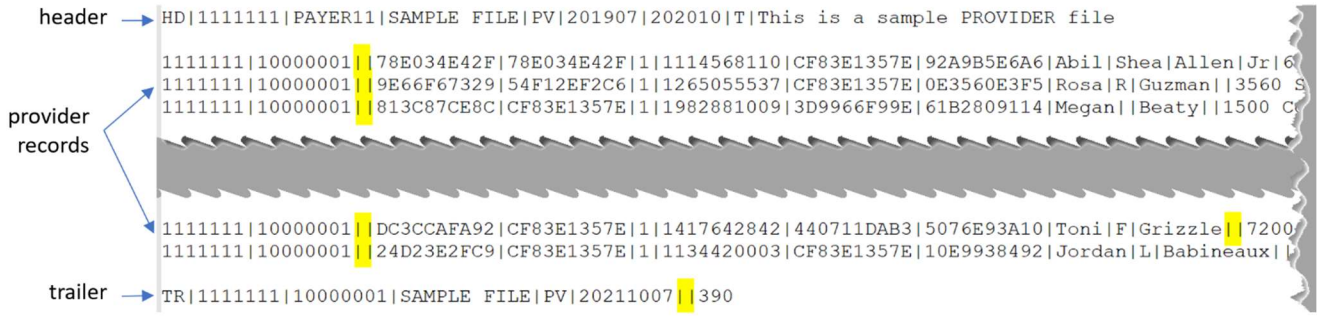
Files to be submitted to the TX-APCD must follow the naming requirements specified in the DSG. It should be noted that there are requirements for naming the raw data files (enrollment, provider, medical, pharmacy, dental), and requirements for naming the package file into which all the raw data files are encrypted and zipped. The following diagram illustrates the naming scheme for both the raw data files and the zip file package.

Figure 3: File Naming Rules



5.2. General Data File Format (with example)

Each data file to be submitted must follow the specifications documented in the CDL and the DSG. In each case, a data file consists of a set of records (rows). At the top of the file is the header record, which is followed by the data records relevant to the specific file type, then ending with the trailer record which summarizes the contents of the file.



The example above is a sample of the provider (PV) file, separated into its component parts: the header record, followed by any number of provider records, and then terminated with the trailer record. It is important to note that every field in the file specification must be accounted for. In the example above, in the case where a field does not have a value, consecutive pipes must be used to indicate the empty value (examples in yellow highlight above).

5.3. Preparing the File Package

The file package is a zip file containing all the data files to be submitted. Any number of tools can be used to create the file package, but the recommended tool is the freeware "7-Zip". If another tool will be used, please read through the requirements below to make sure that the tool you intend to use supports the TX-APCD requirements.

Note: All instructions below are valid as of September 2022 and are just meant as a guide.

If you encounter problems, please refer to the official website of any tools referenced for the most current documentation.

5.3.1. Obtaining the 7-Zip Tool

7-Zip can be downloaded from the 7-Zip website at https://www.7-zip.org/download.html for Windows systems, Linux systems, and macOS systems (terminal version only). It is assumed that the system being used for file preparation is a 64-bit system. Adjust the following instructions accordingly if files are being prepared on a 32-bit system.

- Windows – download the latest 64-bit installation package
- Linux – download the latest 64-bit archive
- macOS – download the only option available

Alternatively, Linux and macOS systems can also use p7zip, which is a command-line only version of 7-Zip.

5.3.2. Installing the 7-Zip Tool

The following are generalized installation procedures for the 7-Zip tool (or an alternate) on each of the three main operating systems. Exact procedures may vary depending on the system, the version being used, and any alternatives that might be available and are not covered in this technical guide.

- Windows – whether the EXE or the MSI installer is downloaded, the installation process is similar. Simply double-click on the install package to execute the installation.
- Linux – the .tar.xz installers available for Linux systems are archives themselves and can be extracted using the standard tar utility in a terminal. For example,

  tar -xf 7z2201-linux-x64.tar.xz -C /home/nixadmin/7zip

  will extract the archive's contents into the indicated 7zip folder. Alternatively, Linux users can install p7zip which is a command-line only version of 7-Zip available for Linux systems. For example, the following command,

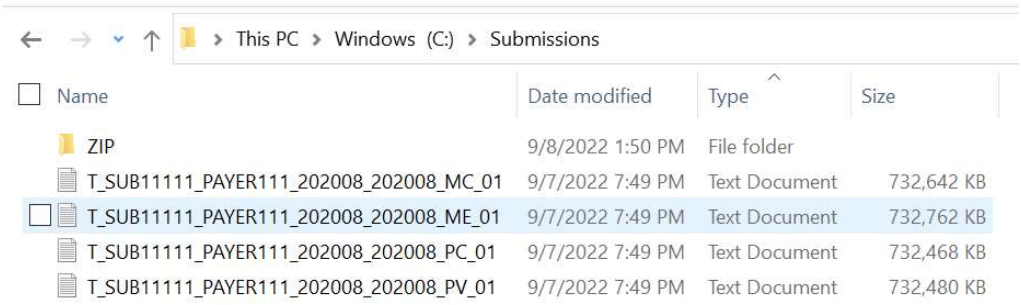
  sudo apt-get install p7zip-full

  will install p7zip on a Debian-based Linux distribution like Ubuntu.
- macOS – follow a procedure similar to the one described above for Linux systems. After downloading the 7z2107-mac.tar.xz archive file, the file can be extracted to access the readme, the user's manual, and the 7zz executable.

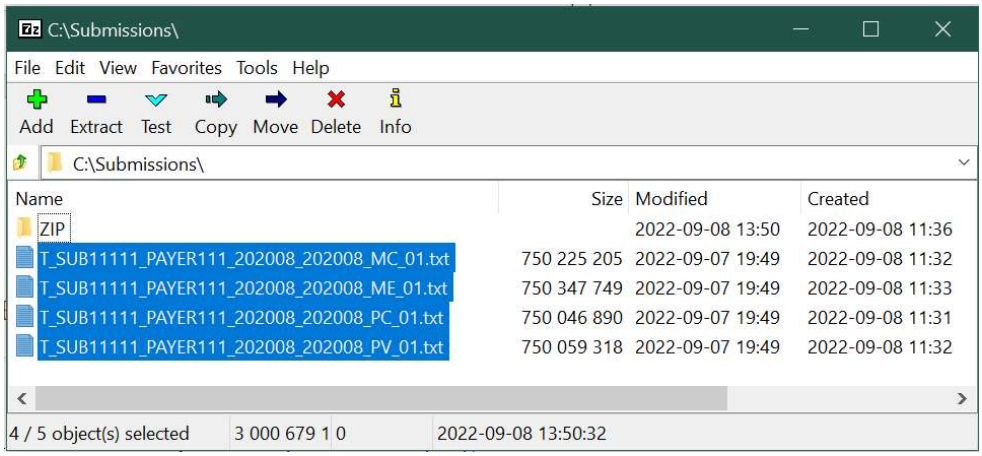
5.3.3. Creating a Zip File Package

Before creating a zip file package, ensure that all raw data files to be submitted are named appropriately according to the instructions in section 5.1. Again, instructions provided here are generalized and can vary slightly across different systems, versions, and alternate tools.

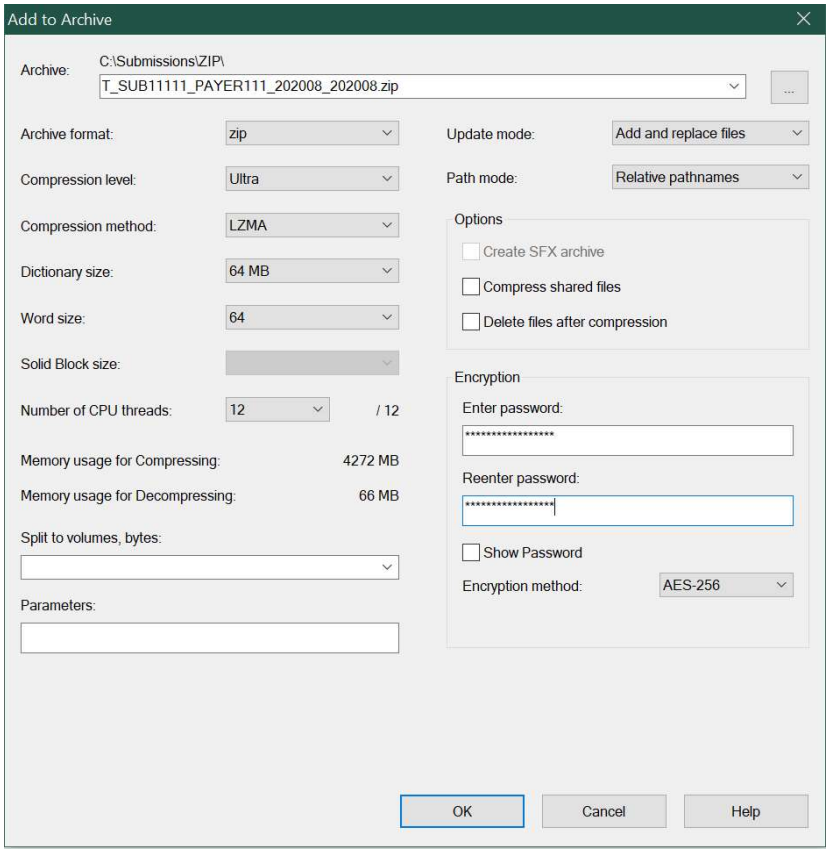
a. Windows – the simplest way to create a zip file package with 7-Zip is to use the graphical user interface (GUI) tool. Suppose, for example, that we want to create a zip file package for the following raw data files:



Simply launch the 7-Zip File Manager and navigate to the location of the data files.



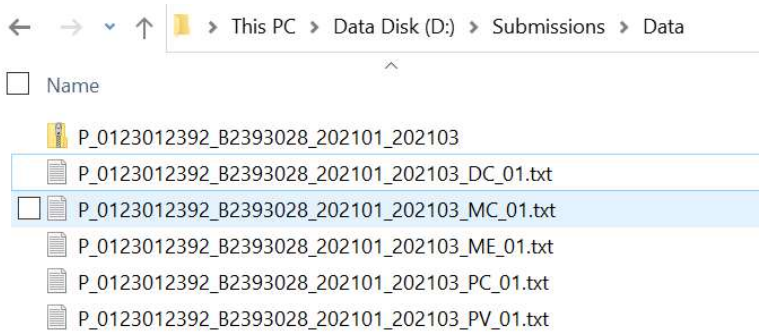
Select the files you want to add to the zip file package and then click the “Add” button to open the Add to Archive dialog which allows you to specify the options for the zip file package being created. Be sure to use the options in the following image to maximize compression and to ensure Advanced Encryption Standard (AES)-256 encryption.



- "Archive" is the name of the zip file package and should be set to the name according to the naming rules described in section 5.1.
- "Archive format" should be set to "zip" (the default).
- Compression level should be set to "Ultra" to get the maximum compression (it will likely take a bit longer).
- Compression method should be set to LZMA.
- "Encryption method" should be set to "AES-256" (the default).
- "Encryption" password (and reenter password) should be populated with the submitter's encryption key that was provided after registration with the TX-APCD as described in section 4.5 of this guide.
- All other options can be left to their defaults.

Click the "OK" button to complete the process and create the zip file package. By default, the zip file will be created in the same directory as the data files (unless a different location is

specified in the “Archive” field at the top of the Add to Archive dialog). For example, the ellipsis button can be used to navigate to a different path where the zip file should be created. In this example, the zip file is created in a subfolder called Data in the Submissions folder.



On the Windows system, the file package can also be created on the command line. Simply open a command prompt (cmd) and change directory to the location of your data:

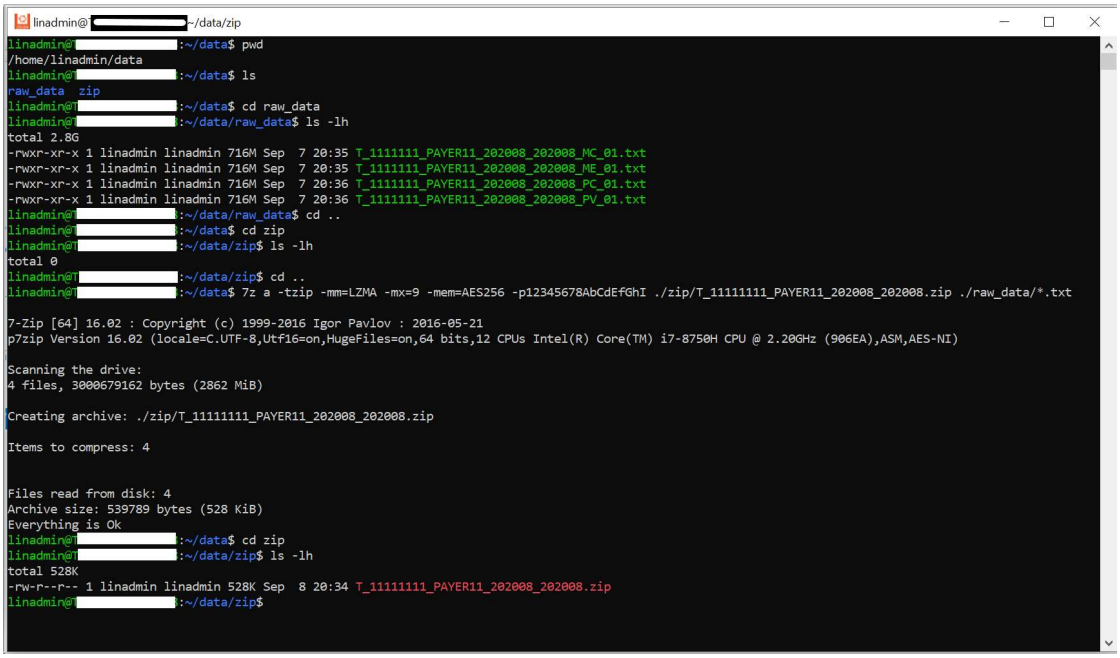
cd “C:/Program Files”

Then the following command can be used to create the zip file package (assumes that the 64-bit version of 7-Zip was installed, and the data is located in C:/Submissions and there is a ZIP subfolder in the Submissions folder):

“C:/Program Files/7-Zip/7z a -tzip -mem=AES256 -m0=lzma -mx=9 -p12345678AbCdEfGh ./ZIP/T_TWOSTEP_87202335_202008_202008.zip *.txt

- The executable has to be quoted because of the space in “Program Files”.
- The -t switch is used to specify the type of archive (zip).
- The -m switch specifies the encryption method (em), the compression algorithm (0) and the level of compression desired (x).
- The -p switch indicates the “password” (the encryption key provided at registration).
- The zip file is being outputted to a subfolder (called ZIP) of the current Submissions folder.
- All .txt files in the current Submissions folder will be included in the zip file package.

b. Linux – the simplest way to create a zip file package with 7-Zip or p7zip is to use the command line in a terminal. In this example, the assumption is made that the p7zip-full package has been installed on the Ubuntu system as described in subsection 5.3.2. Here is a sample terminal session that creates a zip file from a set of raw data files similar to the scenario described above in the Windows example.

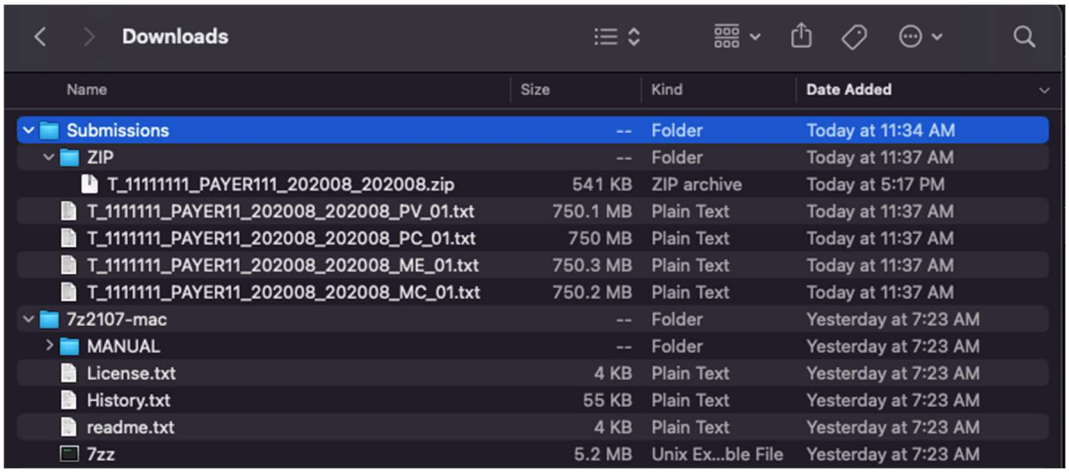


The raw data is in /data/raw_data directory in the user's home directory. The command used to create the zip file package is:

7z a -tzip -mm=LZMA -mx=9 -mem=AES256 -p12345678AbCdEfGhI ./zip/T_TWOSTEP_87202335_202008_202008.zip

- -t specifies the type of archive (zip)
- -mm specifies the compression algorithm (LZMA)
- -mx specifies the level of compression (9 is "Ultra" compression)
- -mem specifies the encryption algorithm
- -p specifies the "password" or encryption key
- the zip file is being created in a subdirectory called "zip" in the current directory
- all .txt files in the raw_data directory will be included in the zip file

c. macOS – creating a zip file package on the macOS is similar to the procedure followed on a Linux system. This example will illustrate the process on macOS. The assumption is made that the raw data files are located in a Submissions folder in the mac user's Downloads folder. Also, the 7z2107-mac.tar.xz archive downloaded from the 7-Zip website has been extracted to the 7z2107-mac folder in the Downloads folder. This structure can be seen in the following image.



Using a zsh terminal, change directory (cd) to the /Downloads/Submissions folder. The following command can then be executed to create the desired zip file package:

../7z2107-mac/7zz a -tzip -mem=AES256 -m0=LZMA -mx=9 -p12345678AbCdEfGhI ./ZIP/T_TWOSTEP_87202335_202008_202008.zip *.txt

Note: The executable being used is 7zz which is the only executable in the macOS installer downloaded from the 7-Zip website.

- -t is used to specify the type of archive (zip)
- -mem specifies the encryption algorithm (AES-256)
- -m0 specifies the compression algorithm (LZMA)
- -mx specifies the level of compression (9 or 'Ultra' compression)
- -p specifies the "password" or encryption key
- the zip file is being created in a subfolder called ZIP and is named appropriately per the rules described in section 5.1. of this guide

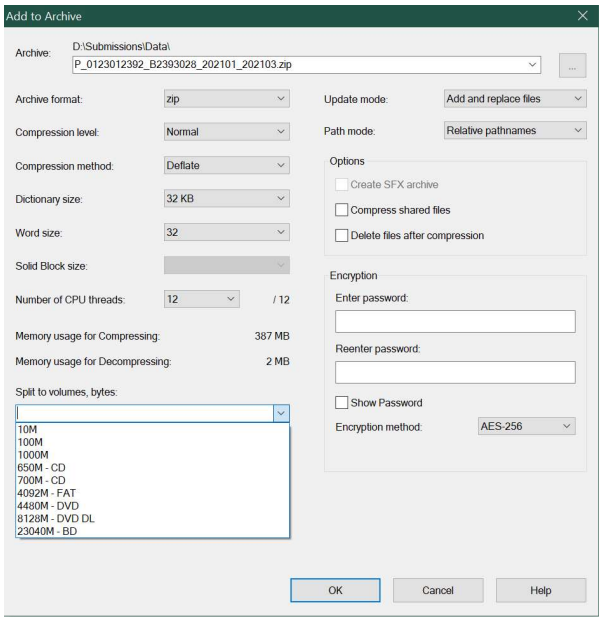
- all .txt files in the current folder will be included in the zip file created

5.3.4. Splitting a Zip File Package

When creating a zip file, one can decide to create a single file or a set of file parts. Splitting the zip file into parts is an old technique that dates back to the period when data was transferred on floppy disks, each of which could only support a specific amount of storage. This technique can be used to split a zip file into parts which can later be reassembled into a single zip file. This could be an option for submitters with low bandwidth internet connections where files may take a long time to transmit.

Note: A split submission will only be processed if and when ALL parts have been successfully submitted.

a. Windows – splitting can be achieved at the time when the zip file package is being created on the Add to Archive dialog by specifying how the file should be split.



In order to facilitate processing, the file should **not** be split into more than 10 parts.

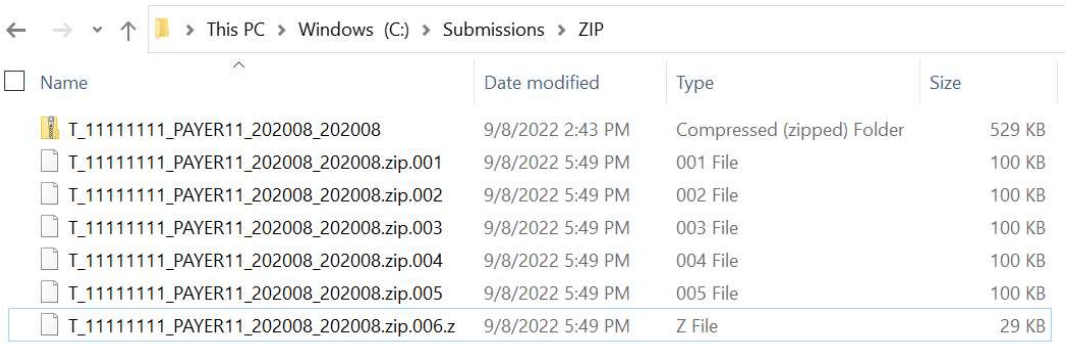
Note: The name of the **final** file part should have a "z" added to the name (reference the relevant section of the Data Submission Guide).

This splitting can also be achieved using the command prompt on a Windows system. Essentially, the v switch can be used to specify the "volumes" or "file parts". For example, we can take the command from 5.3.3(a) and extend it to split the archive.

"C:/Program Files/7-Zip/7z" a -tzip -mem=AES256 -m0=lzma -mx=9 -p12345678AbCdEfGhI ./ZIP/T_TWOSTEP_87202335_202008_202008.zip *.txt -v100k

Note: The -v100k was added to the command from 5.3.3(a).

The effect of this switch is to split the archive into parts no greater than 100 kilobytes. The end result demonstrates the file parts created:



The original zip file is displayed for comparison purposes – the sum of the sizes of the file parts (5 x 100k + 29k = 529k) is equal to the size of the original zip file (529k).

Note: The last file part (006) is modified to add .z at the end as per the naming rules for split files documented in the DSG before being submitted to the TX-APCD for processing.

b. Linux – to split an archive on Debian Ubuntu Linux, the same 7z utility previously used for creating the zip package can be used, simply adding the -v switch to accomplish the splitting of the zip file. The following command will achieve the desired result:

7z a -tzip -v100k -mm=LZMA -mx=9 -mem=AES256 -p12345678AbCdEfGhI ./zip/T_11111111_PAYER111_202008_202008.zip ./raw_data/*.txt

Note: The -v switch which allows the specification of the maximum size of each file part (in this example, 100 kilobytes). The result is the creation of the following files:

```
102400 Sep 21 21:27 T_11111111_PAYER111_202008_202008.zip.001
102400 Sep 21 21:27 T_11111111_PAYER111_202008_202008.zip.002
102400 Sep 21 21:27 T_11111111_PAYER111_202008_202008.zip.003
102400 Sep 21 21:27 T_11111111_PAYER111_202008_202008.zip.004
102400 Sep 21 21:27 T_11111111_PAYER111_202008_202008.zip.005
 27789 Sep 21 21:27 T_11111111_PAYER111_202008_202008.zip.006
```

c. macOS – splitting an archive follows the same pattern as on the Windows platform. Basically, the -v switch can be used to specify the "volumes" that should be created. The same command used in 5.3.3(c) can be extended to achieve the desired result:

../7z2107-mac/7zz a -tzip -mem=AES256 -m0=LZMA -mx=9 -p12345678AbCdEfGhI ./ZIP/T_TWOSTEP_87202335_202008_202008.zip *.txt -v100k

Since this is the same example as has been used throughout, the results are the same.

```
528K Sep  8 17:18 T_11111111_PAYER111_202008_202008.zip
100K Sep  8 21:12 T_11111111_PAYER111_202008_202008_mac.zip.001
100K Sep  8 21:12 T_11111111_PAYER111_202008_202008_mac.zip.002
100K Sep  8 21:12 T_11111111_PAYER111_202008_202008_mac.zip.003
100K Sep  8 21:12 T_11111111_PAYER111_202008_202008_mac.zip.004
100K Sep  8 21:12 T_11111111_PAYER111_202008_202008_mac.zip.005
 28K Sep  8 21:12 T_11111111_PAYER111_202008_202008_mac.zip.006
```

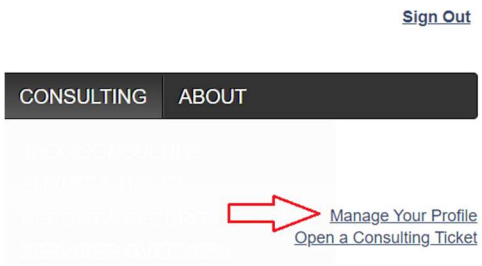
Clearly, the sum of sizes of the file parts is equal to the size of the original zip file.

6.0. Submitting Data to the TX-APCD

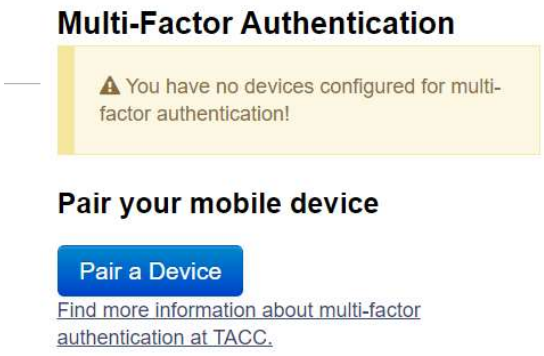
Now that a file package has been created, it can be submitted to the TX-APCD for processing. There are several ways in which file packages can be submitted. They are described in the subsequent sections, in order of preference.

6.1. Setting Up Multi-Factor Authentication on Your TX-APCD User Account

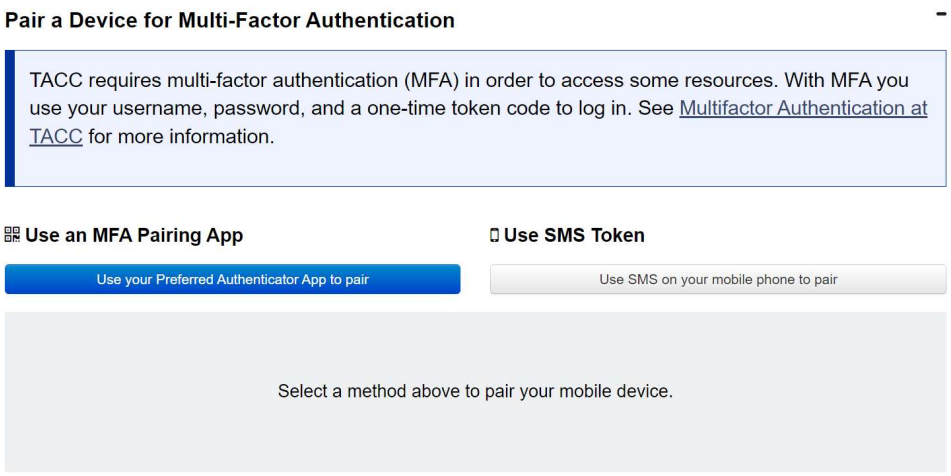
Any attempt to access a resource (SFTP site, website) within the TACC environment requires multi-factor authentication (MFA). To configure MFA for your TACC TX-APCD user account, you need to login to the TACC portal at https://portal.tacc.utexas.edu/home. After logging in, click on the "Manage Your Profile" link which is visible in the upper right corner of the home page.



On the right side of the profile management page, you will see the option to Pair a Device.



You can click on the "Find more information…" link if you want to read more about MFA and how it works. Click on the "Pair a Device" button to proceed.



If you want to find out more about how MFA works at TACC, follow the tutorial on setting up MFA by clicking on the "Multi-factor Authentication at TACC" link. The tutorial walks you through the options with screenshots. As the SMS token is no longer supported, you should select the MFA Pairing App option.

Upon completion, your account profile will show on the right side of the page that your account is MFA-enabled.

Whenever you attempt to log in to a TACC resource (SFTP or website), you will be prompted for your password, and then for a token (in this case, a 6-digit value). You can retrieve the token from your pairing app. Tokens are generated at the time you need them and expire within one minute.

6.2. Secure File Transfer

There are a number of ways in which zip file packages can be securely transferred to the TX-APCD, including command line options and GUI options. This guide will cover some of the well-known and tested methods for securely transferring files over the internet.

6.2.1. Command Line Methods

a. Secure copy (SCP)

SCP is a command line tool that can be used to transfer files securely over the internet. It is available on Linux, MacOS, and Windows (10+) systems. The command syntax is as follows:

scp [local file path] [user]@[host]:[target path]

For example, the following scp command would transfer a file named sample_data.zip from the local machine to the remote TX-APCD submissions folder, for user jdoe555.

scp sample_data.zip jdoe555@secure.corral.tacc.utexas.edu:/corral-secure/projects/APCD/submissions/

Upon executing the command, if it is the first time you are connecting to the Secure Corral storage system at TACC, you will be prompted with the host's fingerprint which you can add to the list of known hosts (and avoid this prompt in future sessions) by choosing "yes" to continue, and "yes" again to add the host to your list of known hosts. You will then be prompted for the password corresponding to the username used in the command (in this example, jdoe555). Finally, you will be prompted for a TACC token which you can retrieve from the MFA app that you associated with your TACC APCD user account in section 6.1.

The copying process will then be executed, with progress reported until the transfer is complete.

b. Secure file transfer protocol (SFTP)

SFTP is another command line tool that can be used to transfer files securely over the internet. Like scp, it is available on Linux, MacOS, and Windows (10+) systems. The command syntax is somewhat similar to scp, but multiple steps are required. First, a connection must be established:

sftp [user]@[host]:[target path]

For example, the following command would start an SFTP session on TACC's Secure Corral storage system for user jdoe555 in the TX-APCD submissions directory.

sftp jdoe555@secure.corral.tacc.utexas.edu:/corral-secure/projects/APCD/submissions/

If the command is successful, the user will be prompted for their password, followed by a prompt for the MFA token as described previously in section 6.1. The user should now be in the console where SFTP commands (SFTP cheat sheet) can be issued to work with files. A file can be uploaded using the ***put*** command. For example, **sftp>** put sample_file.zip, will upload a file called sample_file.zip from the current local directory to the target directory on the Secure Corral storage system. Upload progress would be reported in the console until the file transfer is complete. The ***exit*** command can then be used to disconnect from the Secure Corral system.

6.2.2. Graphical User Interface Methods

The most commonly used GUI tool for file transfer protocol (FTP) and SFTP is FileZilla, a free tool that is available for all major platforms: Linux, macOS, and Windows. Like many popular free tools, FileZilla is often used as a vehicle for spreading malicious code. For this reason, it is important to only download it from the official FileZilla project site, and to check the integrity of the install package after download to validate that it has not been tampered with.

This guide will use FileZilla as an example of how to execute SFTP transfers with a graphical tool. There are many other such tools that can be used. Be sure that the tool you are using comes from a reputable source and was not tampered with prior to installation.

In the case of FileZilla, install packages are available on the official website for 32-bit and 64-bit versions of both Linux and Windows, and also for macOS.

Checking integrity of install package

After downloading the appropriate package for your system, you must also download the available checksums file at the end of the list of downloads. This file can be opened in a text editor and shows the 512-bit checksum for each install package. Open the file and take note of the checksum for the install package you downloaded. The procedure for verifying the checksum

varies across platforms. The examples below assume that the command is executed in the directory where the downloaded file is located. Otherwise, the path would have to be specified as part of the name of the file.

a. Linux – use the sha512sum command. For example,

sha512sum FileZilla_3.60.2_x86_64-linux-gnu.tar.bz2

b. macOS – use the shasum command. For example,

shasum -a 512 FileZilla_3.60.2_macosx-x86.app.tar.bz2

c. Windows – use the certutil command. For example,

certutil -hashfile FileZilla_3.60.2_win64-setup.exe SHA512

In all cases, the output of executing the command will be a checksum which can be compared to the appropriate checksum in the checksum file. If the checksums match, then it is a good indication that the install package has not been tampered with.

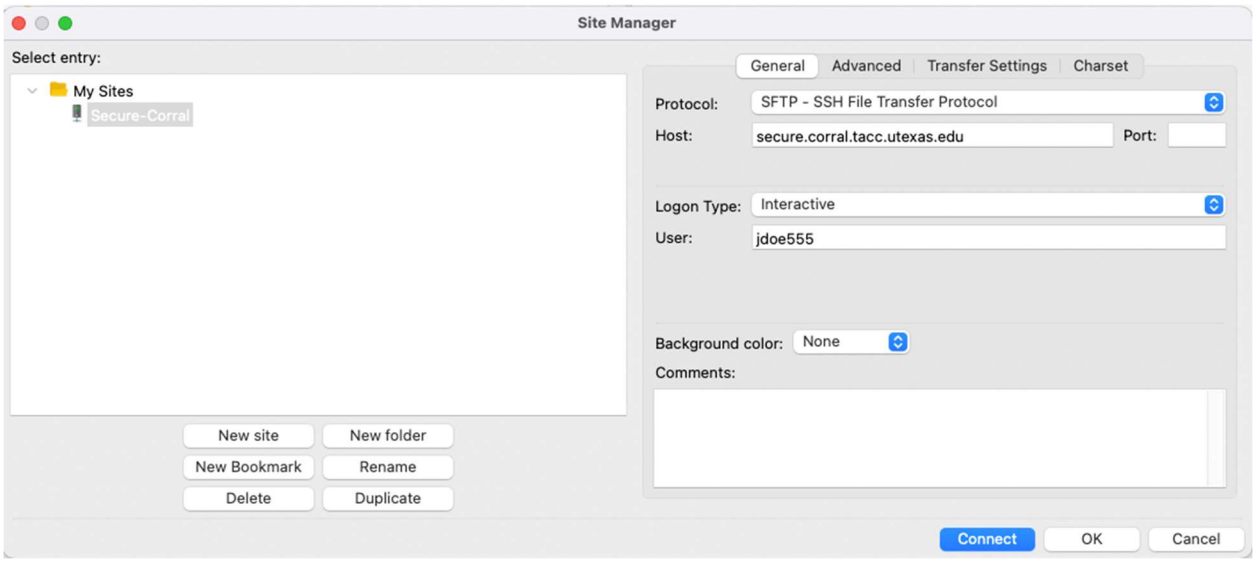
Installing FileZilla

Having verified the integrity of the install package, the package can be installed. Follow the standard installation procedure for your platform. There are no special considerations for installing FileZilla.

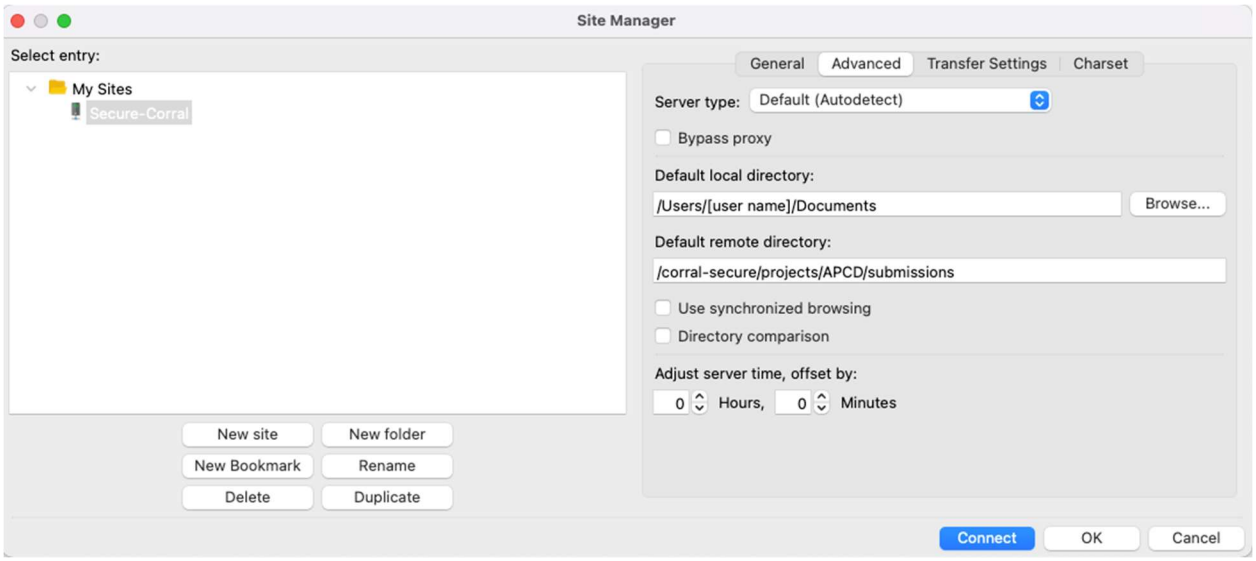
Executing a file transfer using FileZilla

The following series of steps can be used with FileZilla to transfer a file to the TX-APCD. Screenshots used were taken from a macOS environment but are very similar on the other platforms.

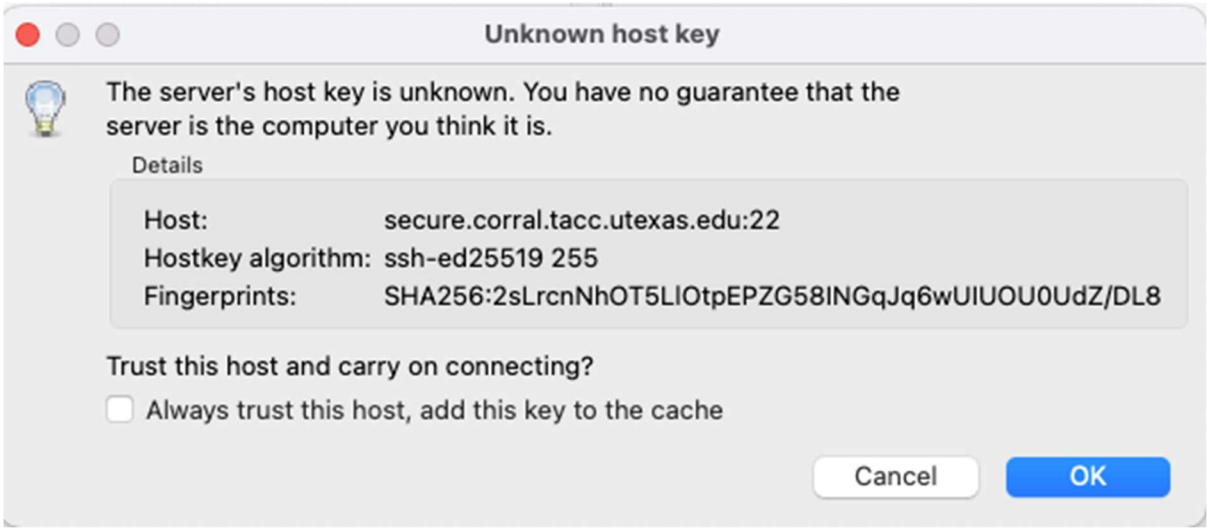
1. Configure the application – start by opening the Site Manager to create a new site. On the General tab, choose ***SFTP*** from the list, and enter ***secure.corral.tacc.utexas.edu*** as the host. The logon type must be set to ***Interactive***. This is because MFA is required to connect (see section 6.1). The user account for the TACC TX-APCD user then needs to be entered as the ***User***.



On the Advanced tab, specify the local directory containing the file to be transferred and the remote directory to which the file should be transferred. In the screenshot below, replace [username] with an actual username.

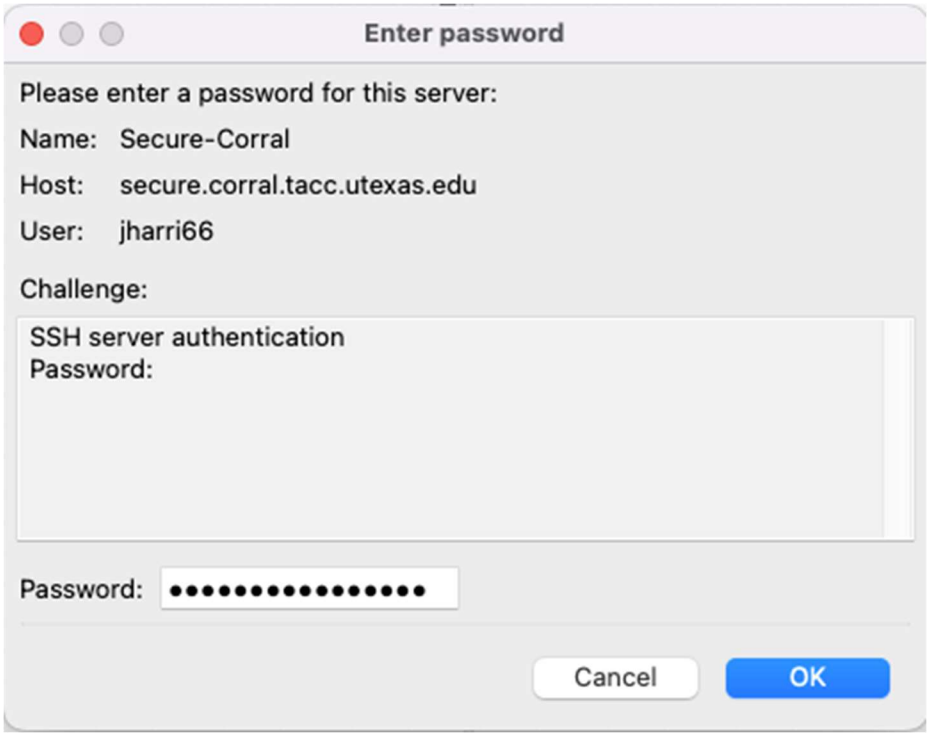


2. Connect to the SFTP site – this is done simply by clicking the “Connect” button. If this is the first time you are connecting to the site, and it has not yet been added as a known and trusted site to the list of local hosts, you will see the following dialog.

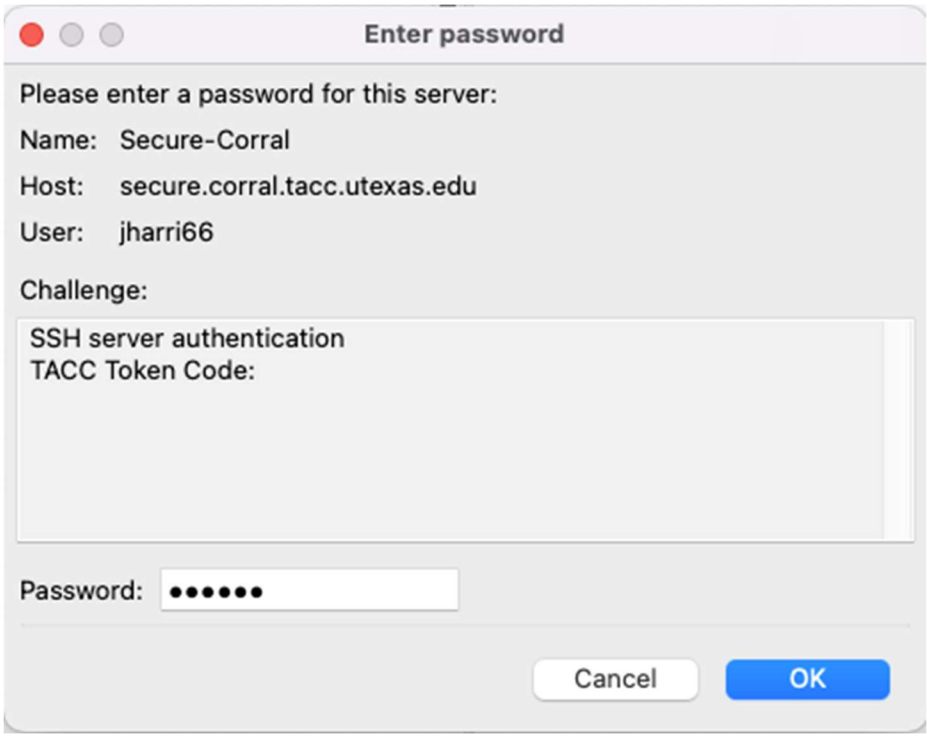


You can choose to trust the remote host and click the "OK" button. You will be prompted each time you connect until/unless you choose to trust the remote host.

Next, you will be prompted for the user's password,



then for the user's token (MFA).



The local directory will be displayed on the left and the remote directory will be displayed on the right.

3. Transfer the file – if the correct local and remote directories were configured in (1) above, then a file from the local directory on the left can simply be dragged and dropped over into the remote directory on the right in order transfer that file. Depending on the size of the file, you may have to wait some time for the transfer to complete. By default, the topmost panel in FileZilla will display a running log of activities including when the transfer is complete.

   Note: You will be prompted for password and token for EVERY file transfer action.

6.2.3. Confirming File Transfer Success

In all the file transfer examples described in this section of the guide, there are three ways to confirm that your file has been transferred successfully:

1. The command line tool or graphical tool used to execute the transfer will provide the result of the operation, indicating whether it was successful or not.

Note: Once the file has been successfully transferred, it will be moved to a different location for processing. This means that a visual confirmation of the transfer will only be possible for a brief period (typically less than 5 minutes).

2. You should receive an email confirming that your file was received and has been queued for processing. This email notification should include general information about the file including its name, time of transfer, and the file's size.
3. All file submission activities are tracked in the submitter administrative portal. The status of a submission is usually visible in the submitter portal within minutes of the submission being received.

6.3. Secure Web Transfer (HTTPS)

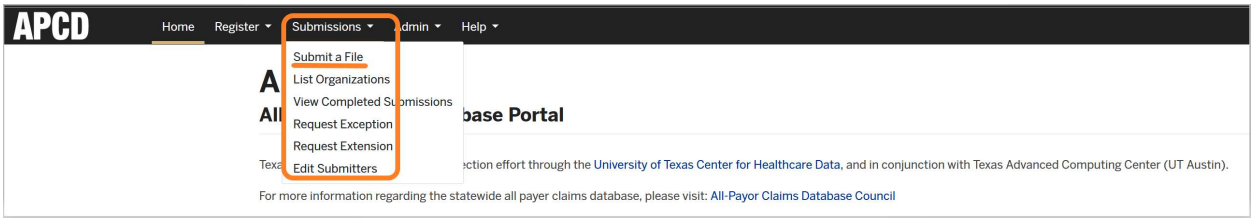
HTTPS is the secure protocol used by default when navigating the internet with an internet browser. In the context of the TX-APCD, secure file transfers can be executed from within the Submitter Administrative Portal (SAP) using an internet browser like Chrome, Firefox, or Microsoft Edge (Chrome is the preferred browser).

6.3.1. Login to the Submitter Portal

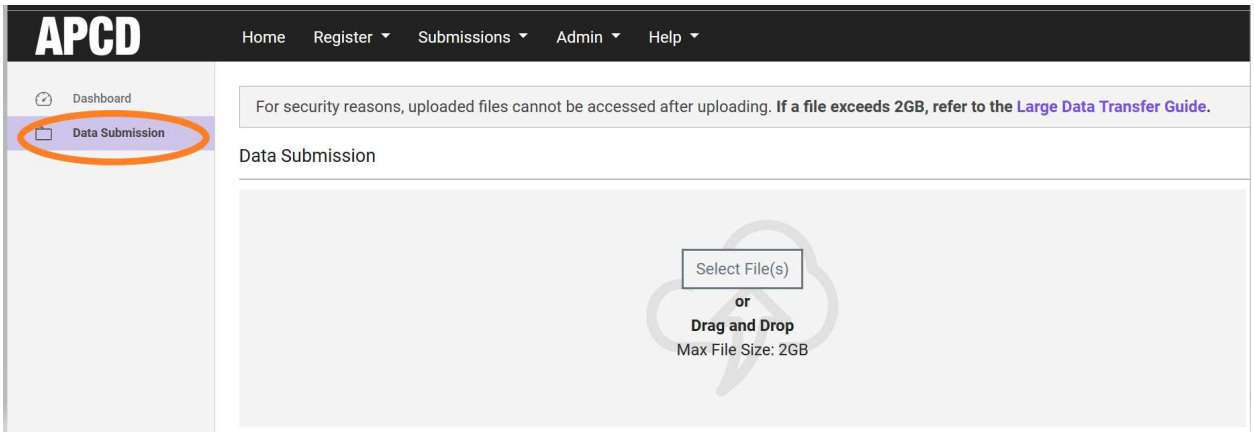
To submit files via secure web transfer (HTTPS), start by clicking the "Login" button at the top right of the page at https://txapcd.org. You will be prompted for your TX-APCD TACC user account name and password. After entering your username and password, you may get an additional prompt (if it is the first time you are accessing the portal) that a portal admin account is requesting permission to access your profile. You can choose the "Approve Always" button to not see this prompt in the future. After logging in, you will be on the portal's home page from which you can access all functionality using the available menus. Your access level to functionality in the portal is based on your role's privileges.

6.3.2. Upload a File Package

To submit a file, start from the Submissions menu item in the top menu bar and choose the "Submit a File" submenu item.



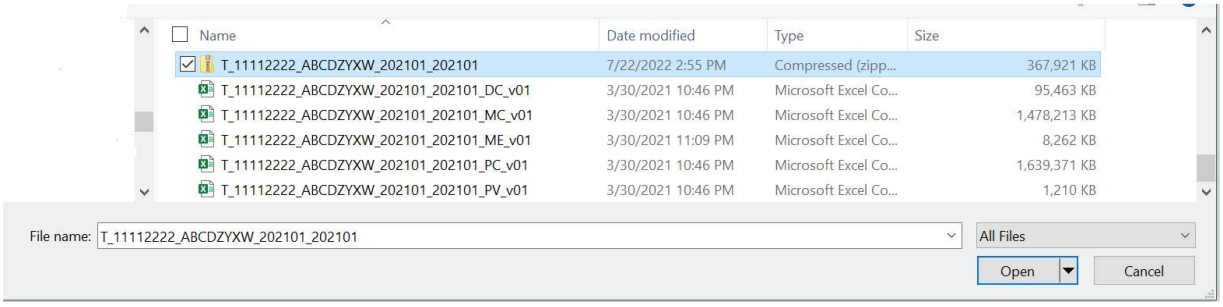
Alternatively, start from the Data Submission item in the menu panel on the left side of the page.



In either case, you will be prompted to select the file you want to upload, or to Drag and Drop the file on to the panel on the right side of the page. You can upload one or multiple files at a time.

Note: There is a limitation currently on the size of web transfers – only files less than 2 gigabytes (GB) in size can be uploaded this way.

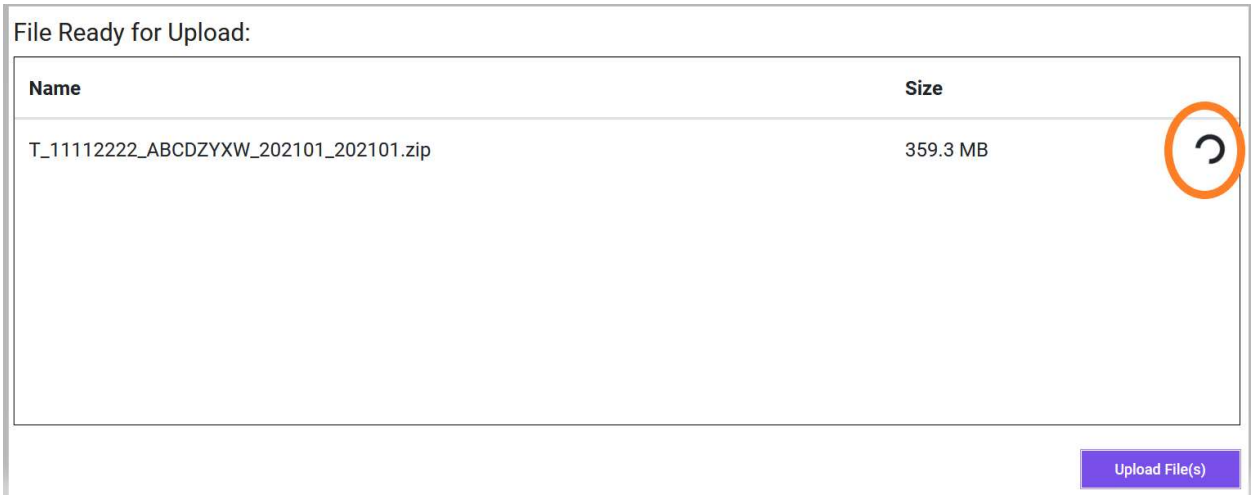
After selecting the file to upload, click on the "Open" button to upload it to the server.



A panel will be displayed in the lower part of the page, and the file you selected will be listed in the File Ready for Upload section.

To upload the file, simply click on the "Upload File(s)" button in the lower right corner of the panel.

You will see a progress indicator on the right side of the file listing.



When the file upload is complete, a SUCCESS message will be visible in the same position where the progress indicator was displayed.

If errors are encountered during this process, please take screenshots of the steps needed to reproduce the error before creating a ticket with the TX-APCD support team.

6.3.3. Confirming Receipt of Transfer

In addition to the SUCCESS message posted on completion of the file upload operation, the methods of file transfer confirmation, listed in 6.2.3, also apply to secure web transfer.

6.4. Encrypted USB Disk

This method allows the submitter to submit files on a USB drive and use a secure courier to deliver the USB drive in accordance with the instructions provided below. In this case, the USB drive should be delivered to the CHCD in Houston. Since this mechanism is very manual and can take some time to execute, it is important to pay close attention to timing to ensure that the submitter remains in compliance with the submission schedule.

6.4.1. Selecting a Secure USB Drive

There are many secure USB drives that can be obtained on the market. The base requirements for USB drives used to transfer data to the TX-APCD include:

- 256-bit AES hardware-based encryption with at least a 6-character key
- Rugged and secure casing
- Compatibility with the Windows operating system (Server 2019+, Windows 10, Windows 11)
- Transfer speed between 5 gigabytes per second (Gbps) and 10 Gbps
- Manufactured to the Federal Information Processing Standards (FIPS) 140-2 standard
- Software-free setup and operation

If in doubt, please contact the TX-APCD operations team to get clarification.

6.4.2. Preparing the Data File(s)

After following the file preparation steps described in section 5.3 of this guide (especially 5.3.3), the file package (ZIP) created can then simply be copied to the USB drive being used for

transfer. The data file package should be zipped and encrypted just as if it were being submitted using one of the online methods (SFTP, HTTPS). In addition to the file package itself being encrypted, the USB drive will provide another layer of hardware encryption to provide further protection if the USB drive is lost or compromised. Neither the encryption key for the physical device nor the encryption key for the file package should accompany the package when it is transferred by the courier. These keys should only be known to the source submitter and the TX-APCD file intake system.

6.4.3. Selecting a Courier

Note: This section is under development and will be published in a future version release of the Technical Guide.

6.4.4. Sending the Package

Before sending the package to the TX-APCD, the submitter must send a notification by email (to submissions@txapcd.org) indicating intent to send the package, along with particulars about the package. The following information is needed:

- The package should be sent to the following address:
  - Adriana Hawkes, CHCD, 1200 Pressler Street 10th Floor, Houston TX 77030
- The email notification sent to the TX-APCD should include the following:
  - The date when the package will be sent along with the anticipated date of delivery to the CHCD in Houston.
  - The encryption key used to encrypt the drive being sent via courier along with any instructions needed for successful unlocking of the drive (which would allow the data file package to be accessed).
  - Instructions on disposition of the USB drive after the data has been retrieved from it. Either the drive can be destroyed by the CHCD, or it can be returned to the submitter. If to be returned, the submitter should arrange for pickup of the USB drive from the same location (and person) where the USB drive was originally delivered.

- The name and contact information for the courier that will be executing the transfer of the package to the CHCD.

6.4.5. Data Transfer to the TX-APCD

After receiving the data package, the CHCD's accountable staff will unlock the USB drive and copy the data file package to secure encrypted storage in the CHCD's data center. The data package will then be transferred to the TX-APCD using the SFTP method. After successful transmission of the data file package to the TX-APCD, the data file package will be permanently deleted from the CHCD's storage. The CHCD's accountable staff will then execute the instructions regarding disposition of the physical USB drive on which the data package was sent.

6.4.6. Confirming Receipt of Transfer

Since the data file package is posted to the TX-APCD using SFTP, the confirmation of receipt of transfer would be the same as for a standard SFTP transfer as documented above in section 6.2.3. However, since the submitter is not the party executing the data upload, the direct visible confirmation provided by the tool being used to do the data transfer will not be visible. Email notifications will be sent as per normal (assuming the submitter has registered contacts who have opted to receive system email notifications). Likewise, submitter personnel with access to the SAP will be able to monitor the status of their submissions through the portal.

7.0. Submission Testing

All submitters are expected and encouraged to submit test files before attempting to submit production data to the TX-APCD. Notification was given on July 11, 2022 of the start of the initial test period on October 10, 2022 extending through the start of monthly data submissions and/or historical data submissions. After the start of regular operations, submitters will continue to be able to submit test files in a number of different scenarios. This section of the guide describes general guidelines for testing both before and after the start of regular TX-APCD operations.

7.1. Submission Definition

For the purposes of this guide, a submission is defined as a single month of adjudicated claims data along with supporting enrollment/eligibility and provider data. For that reason, each submission is tagged with a "data period" which is the time period when the claims were adjudicated and is represented by a CCYYMM value as previously described in this guide.

7.2. Processing of Data Submissions

The processing of data into the TX-APCD can be described in three major stages, each of which includes a start and end point along with a set of activities designed to produce outcomes.

7.2.1. Stage 1

In the first stage, a submission is received and validated primarily for compliance with the CDL specifications and DSG requirements. At the end of this stage, an outcome is determined as to whether the submission is ACCEPTED or REJECTED. In either case, the submitter will receive a detailed report via email notification with a summary of data validation results, including any errors which may have to be corrected before attempting a resubmission.

It is important to note that test submissions are only processed through the end of this stage. The main purpose of testing is to assess compliance of a submission with the specifications and requirements documented in the CDL and DSG, which together ensure a basic level of data quality.

7.2.2. Stage 2

This stage is concerned with three main activities: (a) assessment of data quality beyond the CDL specifications, (b) the deidentification of identified data, and (c) the enrichment of received data with additional information useful to the eventual research use cases of the TX-APCD data.

7.2.3. Stage 3

This is the final stage in which submitted data is staged, normalized, and versioned and then loaded into the TX-APCD data warehouse. It is at this stage that the data finally becomes available for conducting research.

7.3. Identification of Test Submissions

Upon registration, all new submitters are flagged as TEST_SUBMISSION_ONLY. As long as this flag is set on a submitter account, ALL submissions will be considered test submissions and processed accordingly (Stage 1 only). This flag will be removed when a determination is made that testing is complete. This determination is made by agreement between the submitter and the TX-APCD operations team.

After the TEST_SUBMISSION_ONLY flag has been removed from the submitter account, test submissions will be identifiable by the T prefix in the name of the submission file package as described in Section 5.1 of this guide. It should be noted that the TEST_SUBMISSION_ONLY flag may be reapplied at a later date (even after regular submissions have commenced) if the TX-APCD operations team determines that submissions from a particular submitter pose risks to quality in the intake process.

7.4. Test Guidelines

This section provides general guidance for conducting testing.

7.4.1. Current Information

It is incumbent on the submitter to remain abreast of the most current information pertinent to ensure high quality submissions to the TX-APCD. All documentation necessary for building successful submissions can be obtained from the TX-APCD website at https://go.uth.edu/txapcd. At registration, contacts can choose to subscribe to notifications by email which presents a

second way of staying informed. Various industry organizations (for example, TAHP) also disseminate information to their membership, and this presents a third way in which submitters can remain informed of TX-APCD current information.

7.4.2. Purpose

All testing should have a very clear purpose. Tests consume scarce resources and should therefore be done only with very clear expectations in mind. For example, submitting data files that are known to be inconsistent with the CDL and/or DSG requirements is not helpful. Similarly, submitting a single file type when registered to submit four file types is not helpful. Submissions should match the parameters of the submitter's registration (such attributes are part of the submission validation process).

7.4.3. Size

Test files should be only large enough to accomplish the goals of the test. There is no need to submit very large test files (e.g. files containing millions of records) as these will strain available test resources and extend the turnaround time for obtaining test feedback. The goal of the test environment is to provide feedback within 48 hours of receipt of a submission. However, this is only an aspirational goal since it must be achieved within the context of resource constraints. The bottom line is that test files should be only as large as they need to be so that feedback can be obtained in a timely fashion.

7.4.4. Frequency

There is no limit on the frequency of test submissions. However, it is assumed that purposeful submissions would allow for time to obtain and analyze feedback from one test before planning and executing a follow-up test. It is hard to imagine, for example, a scenario where multiple test submissions in an hour would be helpful (to the submitter or the TX-APCD). As in the case of the guidance on size, test submissions should be made as frequently as necessary, but not more than.

7.4.5. Success

To determine whether testing has been completed as successful is ultimately made by the TX-APCD operations team in collaboration/consulting with the submitter. A general rule of thumb is

at least two consecutive accepted test submissions would be indicative of successful test completion. An accepted test submission is one which has passed the Stage 1 validation process (and under regular monthly production protocol, would proceed to Stage 2).

APPENDIX A – Abbreviations/Acronyms Used

Description	Abbreviation/Acronym
Acceptable Use Policy	AUP
Administrative services only	ASO
Advanced Encryption Standard	AES
Center for Health Care Data	CHCD
Centers for Medicare and Medicaid Services	CMS
Certified Qualified Entity	QE
Change directory	cd
Command prompt	cmd
Common Data Layout	CDL
Data Submission Guide	DSG
Encryption method	em
Federal Information Processing Standards	FIPS
File Transfer Protocol	FTP
Gigabytes	GB
Gigabytes per second	Gbps
Graphical user interface	GUI
High performance computing	HPC
Hypertext Transfer Protocol Secure	HTTPS
Multi-factor authentication	MFA
Portable document format	PDF
Provider	PV
School of Public Health	SPH
Secure copy	SCP
Secure File Transfer Protocol	SFTP
Submitter Administrative Portal	SAP
Texas Advanced Computing Center	TACC
Texas All-Payor Claims Database	TX-APCD
Texas Department of Insurance	TDI
Third party administrator	TPA
Universal Serial Bus	USB
University of Texas Health Science Center at Houston	UTHealth Houston