Texas All-Payor Claims Database

Technical Guide

January 21, 2025

Version 2025.01

UTHealth
The University of Texas
Health Science Center at Houston

School of Public Health | Center for Health Care Data

1200 Pressler | Houston | TX 77030

Ph: 713.500.9000 | https://go.uth.edu/txapcd

Table of Contents

1.0. Document Version History

VERSION HISTORY		
Version Number	**Date Published**	**Summary of Revisions**
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.
2023.05.a	5/17/2023	Draft of second edition
2023.05	5/23/2023	Second published edition
2025.01	1/21/2025	Third published edition (release of CDL v3.0.1)

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. As the 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. Complimentary Documentation

Before working with this technical guide, please be sure to download and review both the Data Submission Guide (DSG), the Common Data Layout (CDL), and any accompanying Errata. The Data Submission Guide provides an overview of the function of the APCD in terms of expected submitters, registration process, submission schedules, structure of submissions, and submission process. The Common Data Layout provides information on the specific data files, data fields, and expectations about field values, data formats, etc. These documents lay the foundation for this technical guide and the three documents are intended to be used together. In the event of overlapping guidance between the Technical Guide and the DSG, submitters are expected to follow the guidance provided in the Technical Guide.

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.

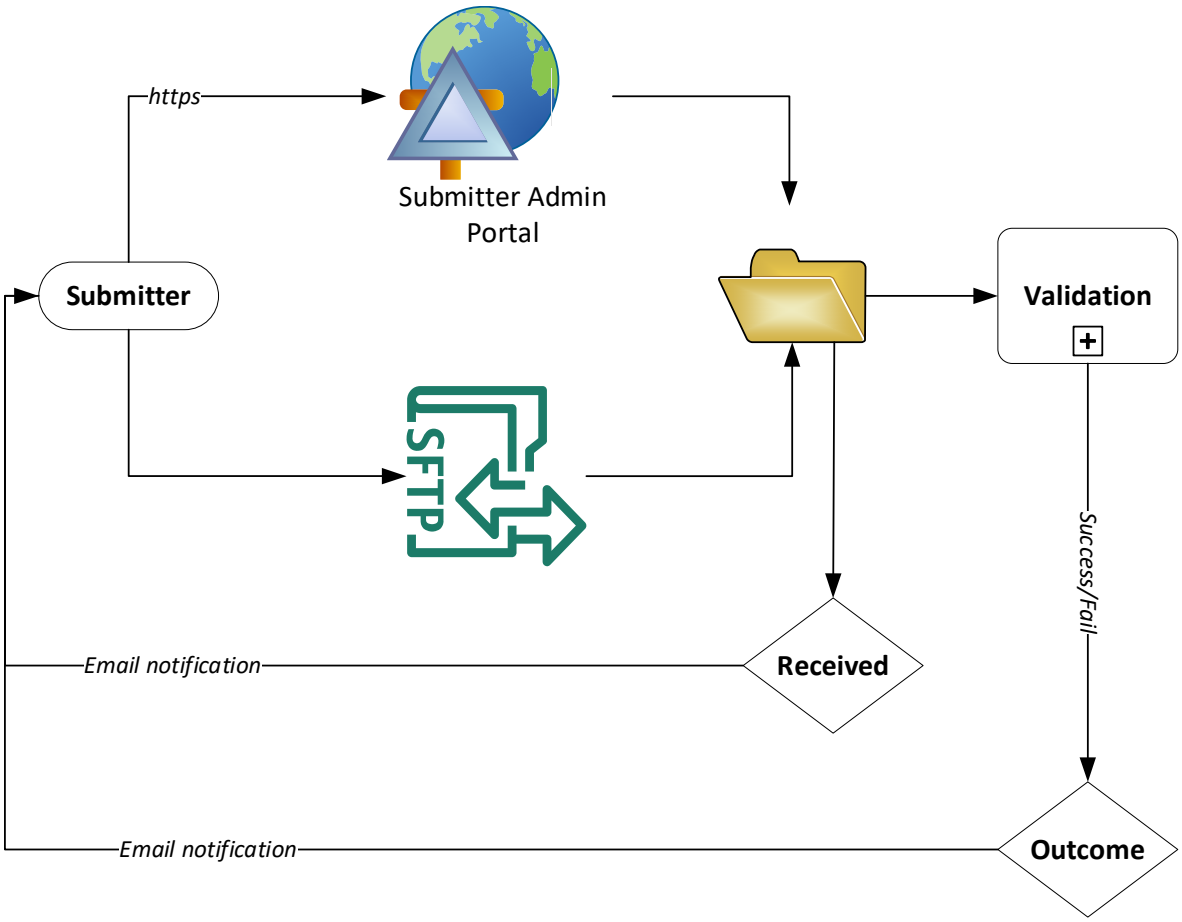
Topics to be covered include:

(a) how to register your organization with the TX-APCD
(b) how to obtain a submitter identity and encryption key
(c) how to obtain a TX-APCD user account
(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

(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.

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.

Following a successful submission, submitters should expect to receive two emails from the TX-APCD.

- The first email (Subject: 'Submission Receipt Notification') will confirm that the package has been received and will include feedback on the structural integrity of the package.
- The second email (Subject: 'Submission Validation Notification') will include the results from the file validation process. Submitters can subscribe to these notifications when registering their organization with the TX-APCD.

Figure 2 – Validation Process

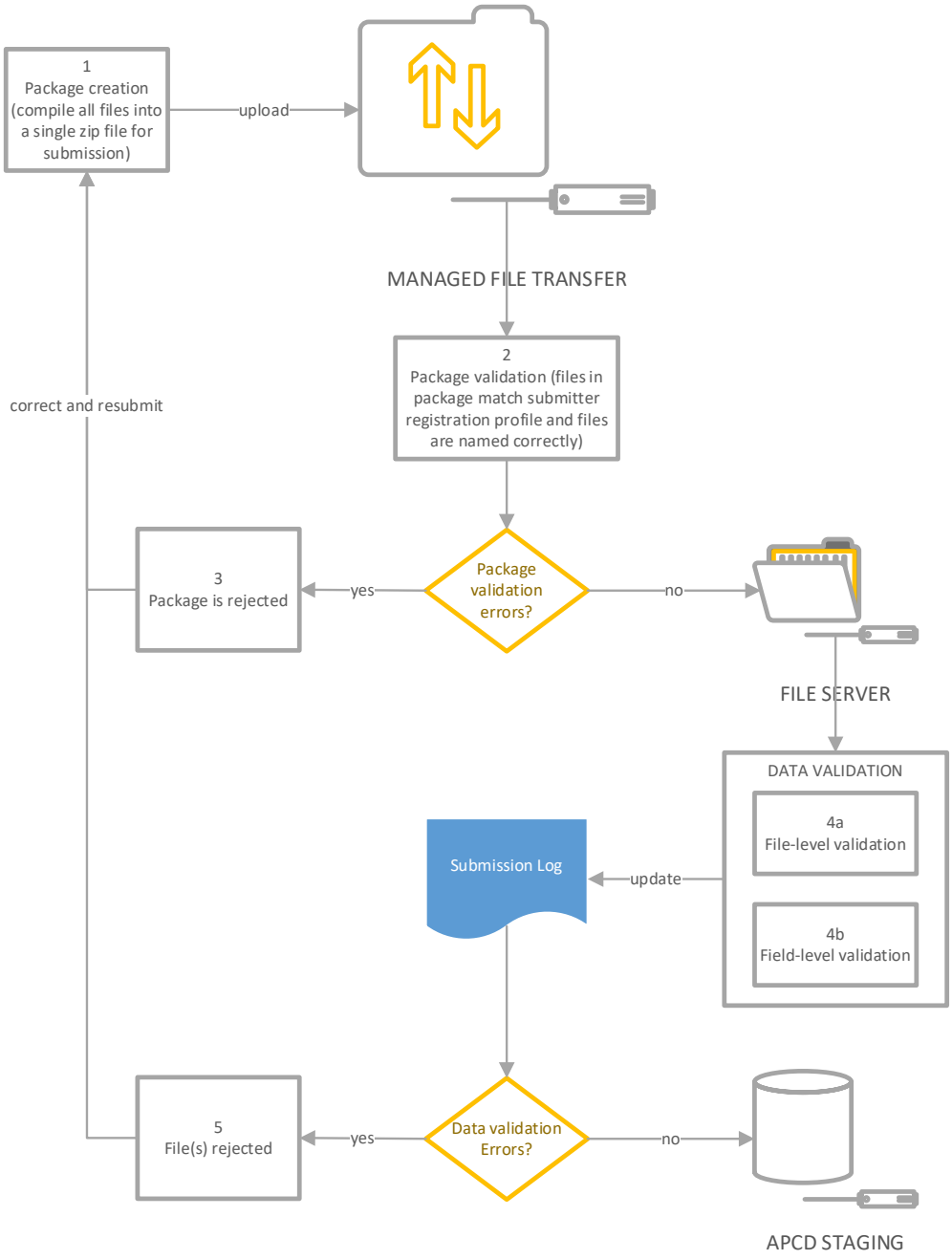


Figure 2 describes the validation process. A successful file validation process only indicates that the file contents are consistent with the rules specified in the CDL. Subsequent checks will be performed to ensure that the data is semantically consistent.

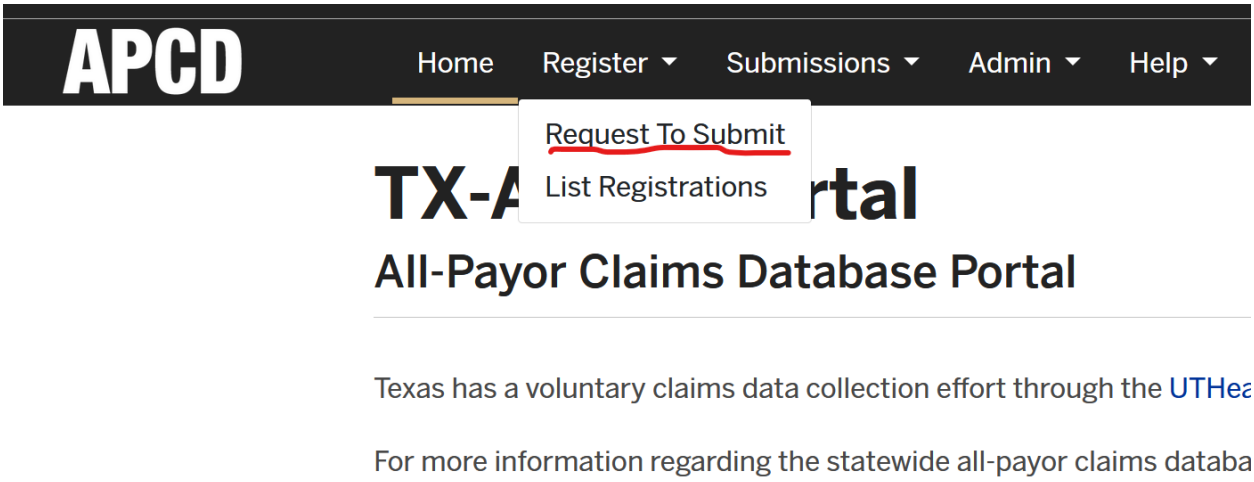
3.0. Registration

Organizations must be registered with TX-APCD 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.

3.1. Online Registration (Preferred)

The preferred method for registering (or renewing a registration) with the TX-APCD is the submitter portal (https://txapcd.org).

(a) After logging into the submitter portal, use the Register menu to Request to Submit



(b) **Organization** section: be sure to enter the correct year (the year during which submissions will be made). Business name and address should reflect official business name and address of the organization.

(c) **Entity** section: add information for all the business entities which are offering healthcare plans in Texas. Add as many as necessary.

(d) **Contact Information** section: contact information for individuals in your organization who are responsible for some aspect of your organization's

submissions. Add as many as necessary. Note the checkbox to receive system notifications. Please make sure your organization whitelists the domains uth.tmc.edu and tacc.utexas.edu to allow emails.

3.2. Offline Registration (Deprecated)

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. Complete the registration 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.

3.3. Registration Notes

All carriers that do business in Texas will need to register with the TX-APCD; there are no exceptions. The same applies for plan administrators (third party administrator [TPA]/administrative services only [ASO]) and pharmacy benefit managers (PBMs) who may be submitting data on behalf of any health plans within the scope of the law.

Submitters may request extensions if unable to meet the submission schedule; or exceptions if they cannot meet a requirement of the rule.

Eligibility for exceptions and/or extensions cannot be determined until registration is successfully processed. Section 3.6 of this guide outlines how to request an exception or submission date extension.

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 calendar year (or as directed by the TX-APCD) 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

To avoid the rejection of emails sent to you, 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. If you believe your encryption key has been compromised in any way, please request a replacement as soon as possible.

For submitters using GPG for file encryption, please consult Appendix B.

3.4. Submitter Identifiers

In this guide, the term "submitter" will be used to represent an overall organizational entity. The "payor" will refer to the company, subsidiary, business unit or plan which will submit 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 "payors" should be created for the registering submitter. If a single organization has multiple subsidiaries/units doing business in the state, then each subsidiary/unit may qualify as an individual payor. There could be other reasons why multiple "payors" might be established for a registering organization. The determination of how many payors are needed for a given submitter will be made by the TX-APCD operations team in consultation with the registering organization.

For the purposes of illustration in this guide, we will use a hypothetical submitter. The organization is named Two Step Insurance Company, which has a medical plan and a separate dental plan.

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

(1) Submitter Code – this is an alphanumeric code that identifies the overall organization and is no more than 8 characters in length, in the form of a mnemonic of the organization's name. For example, Two Step Health Insurance company is assigned the submitter code TWOSTEP.
(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 is assigned the payor codes 50000010 for their medical plan and 50000011 for their dental plan. It is important to note that both the submitter

code CDLXX001 and the payor code CDLXX002 are mandatory across all data file types.

3.5. Encryption Keys

Data files submitted to the TX-APCD must be zipped and encrypted. As part of the registration process, a unique encryption key is assigned to each payor code issued. The encryption key must be used to encrypt the data file package (ZIP file) 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. For submitters using GPG encryption, please consult Appendix B.

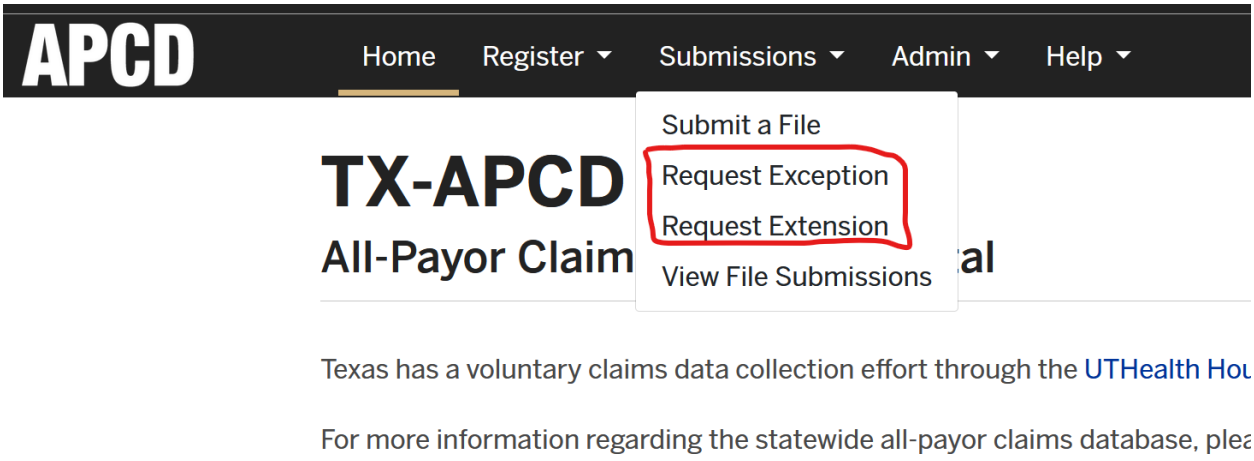
The TX-APCD reserves the right to assign a new encryption key to a submitter periodically, with at least 45 days of notice before the new key is required for new submissions. A submitter can also request a new encryption key if the assigned key has been compromised. Please send the request to txapcd@uth.tmc.edu.

3.6. Extensions and Exceptions

Submitters may request extensions and/or exceptions as needed. An extension is required if a submitter is unable to meet the submission schedule as defined in the Rule. Small payors with less than 10,000 covered lives may request the small payor extension if more time is needed to comply with the law.

Exceptions may be requested if the submitter is unable to comply with one or more requirements of the Rule. The most common use case for exceptions are threshold exceptions where a submitter is unable to meet the threshold requirement for one or more fields specified in the CDL.

Extensions and exceptions can both be requested on the TX-APCD submitter portal (https://txapcd.org) under the **Submissions** menu. This is the preferred method for requesting both extensions and exceptions.



The request forms are also available in PDF format and include instructions on how to complete and submit the requests. To request either, navigate to https://go.uth.edu/txapcd and open the TX-APCD Payor Registration and Information sub-menu. The forms can be downloaded, completed, and then submitted to the general TX-APCD mailbox (txapcd@uth.tmc.edu).

4.0. Obtaining a TACC TX-APCD User Account

A TACC user account is required to access computing resources and submit files to TX-APCD. 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.

4.1. 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 an organizational 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 to which you belong.

(4) Submit the form by clicking on the "Create TACC Account" button.

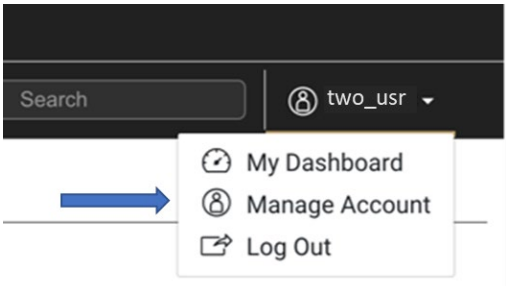
(5) Check the mailbox for the email you specified in the request. You should receive an email titled "TACC Account Action Required: AUP confirmation" containing a link to TACC's Acceptable Use Policy (AUP). Click the link to view the AUP.

(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.

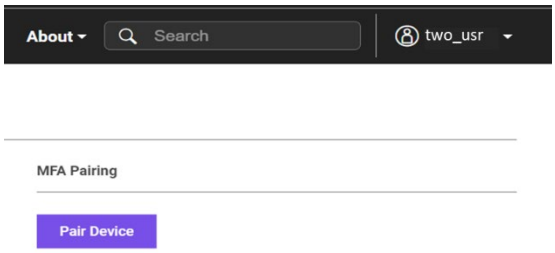
(7) Your account will be reviewed, and you should receive a response to your account request within two business days.

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

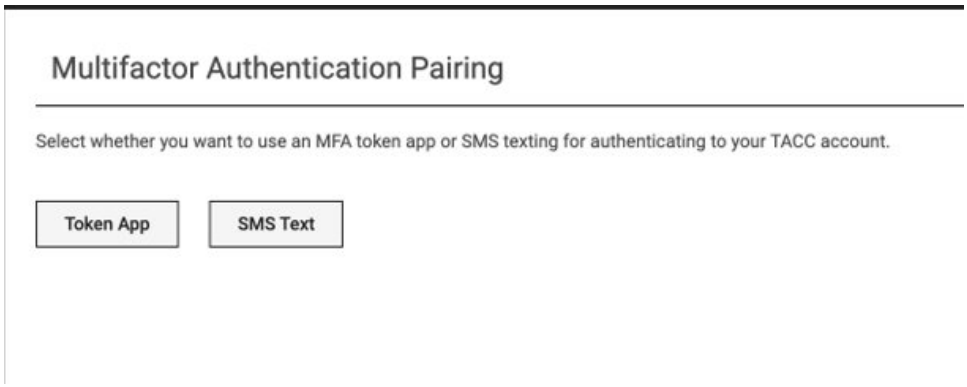
Any attempt to access a resource (SFTP site, website) within the TACC environment requires multi-factor authentication (MFA). To configure MFA for your TACC TX-APCD user account, you need to login to the TACC portal at https://portal.tacc.utexas.edu/home. After logging in, click on the "Manage Account"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

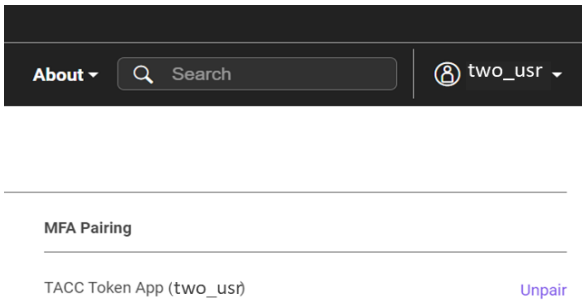


Click on the “Pair Device” button to proceed.



If you want to learn more about how MFA works at TACC, follow the tutorial on setting up Multifactor Authentication (MFA) at TACC at the following link https://docs.tacc.utexas.edu/basics/mfa/. The tutorial walks you through the options with screenshots. You may choose to authenticate with Standard SMS text messaging or Token application. We would recommend selecting MFA Token App, as it may take some time for the text message to reach you.

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 chosen authenticator app such as Google Authenticator or Duo. Tokens are generated at the time you need them and expire within one minute.

5.0. 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 as necessary. This section of the guide describes general guidelines for testing both before and after the start of regular TX-APCD operations.

5.1. 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 guidance on the specific data field expectations for each data file type, please refer to the Common Data Layout (CDL) and accompanying Errata.

Each submission is tagged with a "data period" which is the time period when the claims were adjudicated and is represented by a CCYYMM (ex. 201901 for January 2019) value as previously described in this guide.

- The medical, dental, and pharmacy claim files are abbreviated as MC, DC, and PC, respectively. These files should include all adjudicated claims within the monthly submission.
- The eligibility file is abbreviated as ME and includes all subscriber and member enrollment information. This file should include all persons eligible for plan benefits.
- The provider file is abbreviated as PV (not MP) and includes all in-network contract providers associated with the plan within the state of Texas. Additionally, the file should contain provider information on all providers that have had a claim adjudicated during the reporting period.

For the Two Step Health Insurance Company with submitter id: TWOSTEP and payor code: 50000010, the submission of January 2022 data is the following zip file package:

T_TWOSTEP_50000010_202201_202201.zip

T_TWOSTEP_50000010_202201_202201_ME_01.txt

T_TWOSTEP_50000010_202201_202201_PV_01.txt

T_TWOSTEP_50000010_202201_202201_MC_01.txt

T_TWOSTEP_50000010_202201_202201_PC_01.txt

Please note that a zip file includes all data files that Two-Step Health Insurance Company registered to submit.

5.2. 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.

5.2.1. 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 PASSED or FAILED. 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.

5.2.2. 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.

There may be scenarios where data quality issues are detected in this stage and submitters contacted to investigate the nature of those issues. In such cases, a corrected resubmission might be warranted.

5.2.3. 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.

5.3. Identification of Test Submissions

Upon registration, all new submitters are flagged as TEST_SUBMISSION_ONLY. If 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 and the TX-APCD moves into production operations. This determination is made by agreement between the submitter and the TX-APCD operations team. Section 5.4.5. of this Technical Guide further discusses the testing completion requirements and procedure.

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 6.1 of this guide. It should be noted that the TEST_SUBMISSION_ONLY flag may be reapplied later (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.

5.4. Test Guidelines

This section provides general guidance for conducting testing.

5.4.1. 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.

5.4.2. Purpose

All testing should have a very clear purpose. Tests consume scarce computing 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 usually not helpful. Similarly, submitting a single file type when registered to submit four file types will result in the package not being accepted for validation. Submissions should match the parameters of the submitter's registration (such attributes are part of the submission validation process).

5.4.3. Size

Test files should only be 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 useful feedback can be obtained in a timely fashion.

5.4.4. Frequency

There is no limit on the frequency of test submissions. However, it is assumed that purposeful tests 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). It is very likely that most test submissions will suffer from the same issues. Feedback on those issues can be obtained as well with one or two test files as

with twenty test files. As in the case of the guidance on size, test submissions should be made as frequently as necessary, but no more.

5.4.5. Success

The determination of whether a submitter's testing has been completed successfully is ultimately made by the TX-APCD operations team in collaboration/consultation with the submitter. The TX-APCD recommends submitters have at least two separate months of accepted zip file submissions in which all data files pass validation. 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).

If a submitter believes they have completed testing, they should notify the TX-APCD support team by submitting a support ticket titled 'TESTING COMPLETE' using your TX-APCD user account at https://txapcd.org/. In the ticket, the requestor should indicate the payor code(s) they are reporting a completed with testing. The TX-APCD will confirm if the payor code has completed minimal testing requirements described above. If determined to be complete, the requestor will be issued a 'Testing Complete' certificate and have the TEST_SUBMISSION_ONLY flag removed from the payor code (assuming production operations have commenced). The TX-APCD reserves the right to request additional test submissions if needed.

6.0. 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.

6.1. File Naming Requirements (with example)

Files to be submitted to the TX-APCD must follow the naming requirements specified in the DSG (and Errata). It should be noted that there are requirements for naming the raw data files (enrollment ME, provider PV, medical MC, pharmacy PC, dental DC), and requirements for naming the ZIP package file into which all the raw data files are

encrypted and zipped. The following diagram illustrates the naming scheme for both the zip file package and the raw data files.

Figure 3 – File Naming Rules

ZIP file name: T_TWOSTEP_50000010_202201_202201.zip

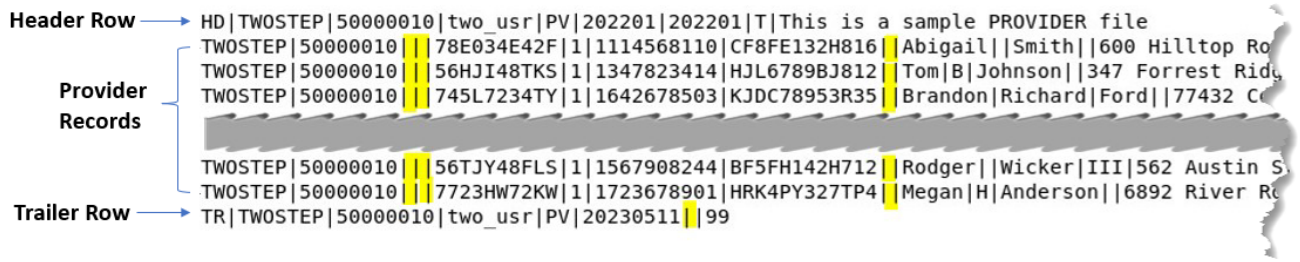
Indicates TEST or PRODUCTION file (T/P)	Submitter code	Payor code	Data period start month in CCYYMM format	Data period end month in CCYYMM format
T	TWOSTEP	50000010	202201	202201

Raw eligibility data file name: T_TWOSTEP_50000010_202201_202201_ME_01.txt

Indicates TEST or PRODUCTION file (T/P)	Submitter code	Payor code	Data period start month in CCYYMM format	Data period end month in CCYYMM format	Type of data file (ME, PV, MC, PC, or DC)	File version number (in the case of resubmitted files)
T	TWOSTEP	50000010	202201	202201	ME	01

6.2. General Data File Format (with example)

Each data file to be submitted must follow the specifications documented in the CDL, DSG, and their Errata. In each case, a data file consists of a set of rows. The first row in each file is the header row (HD) which is followed by the data records relevant to the specific file type, then ending with the trailer row (TR) which summarizes the content of the data file. 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 row, followed by any number of provider data rows, and then terminated with the trailer row. It is important to note that every field in the file specification must be accounted for. Consecutive pipes (|| with no spaces) must be used to indicate the empty/null values as highlighted in the above example.

Note: Only three types of rows should be present in each data file type: a header row, data row(s), and a trailer row. There is no need to include a row of field labels anywhere in the file.

6.3. 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 May 2023 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.

6.3.1. 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.

6.3.2. 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/[user]/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,

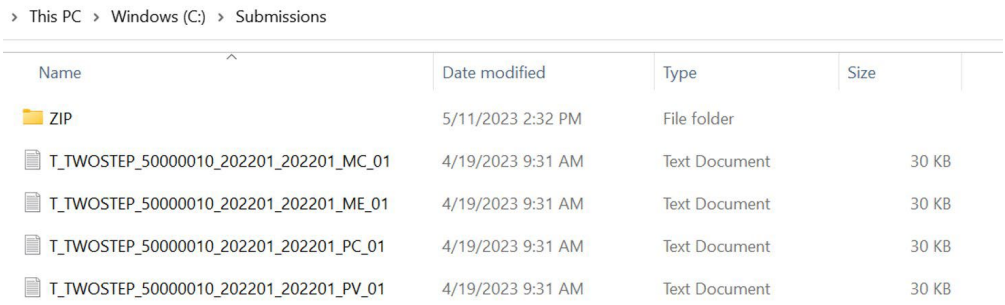
  sudo apt-get install p7zip-full

  will install p7zip on a Debian-based Linux distribution like Ubuntu.
- macOS – follow a procedure like 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.

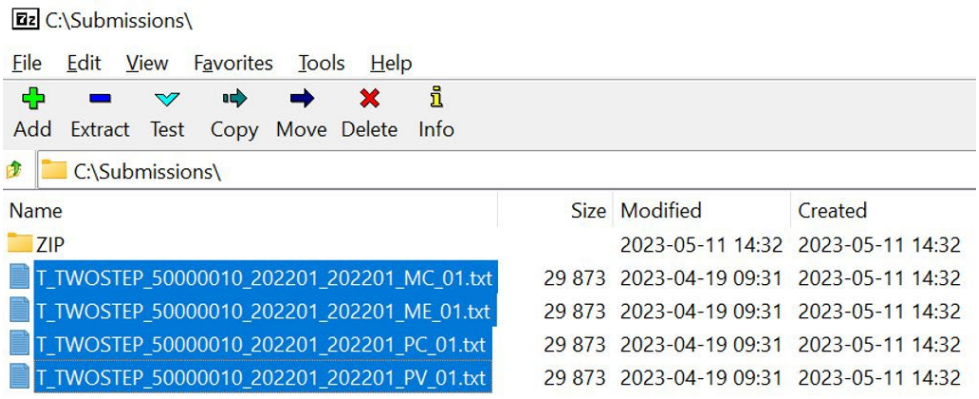
6.3.3. Creating a Zip File Package

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.

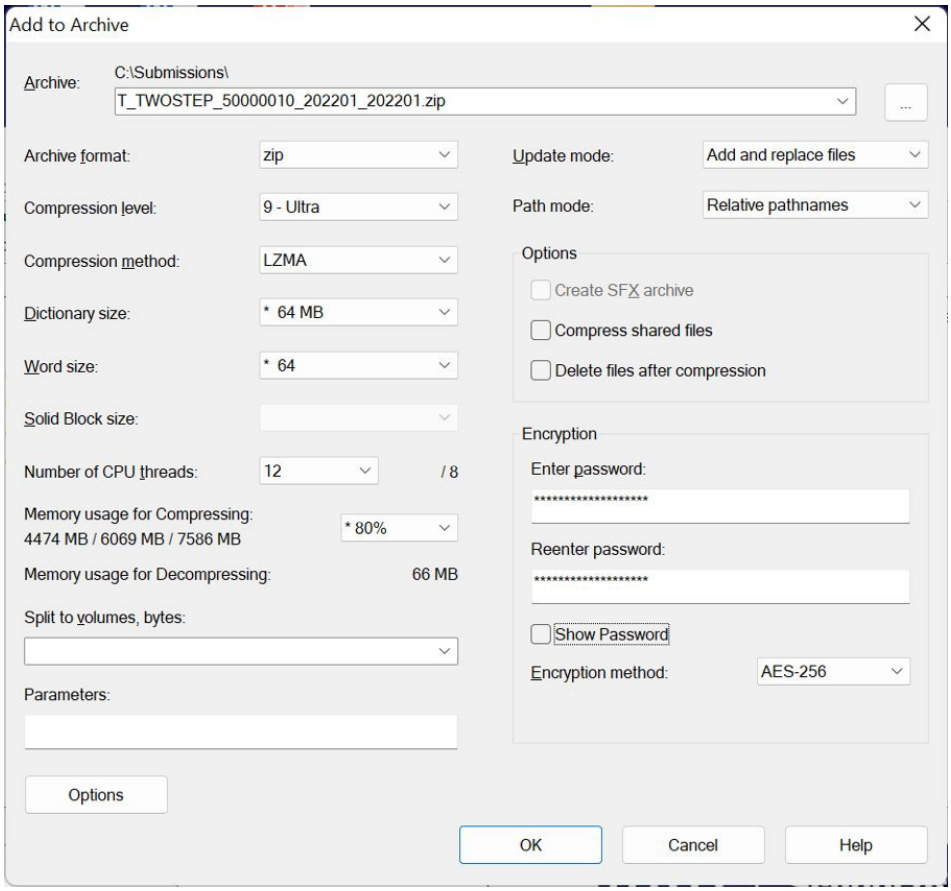
a. Windows – the simplest way to create a zip file package with 7-Zip is to use the graphical user interface (GUI) tool. Suppose, for example, that we want to create a zip file package for the following raw data files:



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

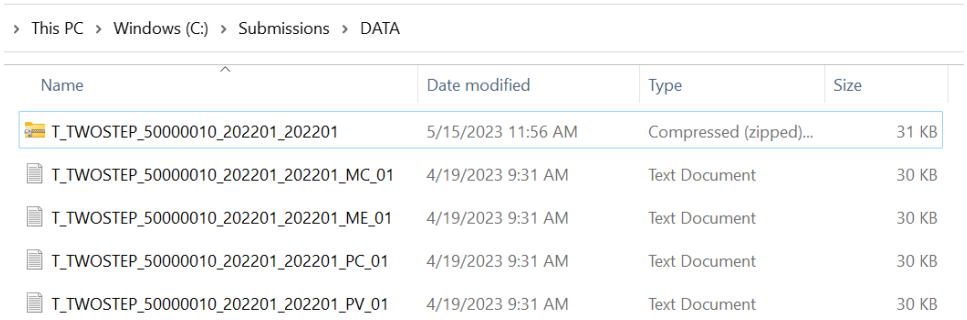


Select the files you want to add to the zip file package and then click the "Add" button to open the Add to Archive dialog which allows you to specify the options for the zip file package being created. Be sure to use the options in the following image to maximize compression and to ensure Advanced Encryption 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. Assuming that the data files are in C:/Submissions and there is a ZIP sub-folder in the Submissions folder, then open a command prompt (cmd) and change directory to the location of your data:

```
cd "C:/Submissions"
```

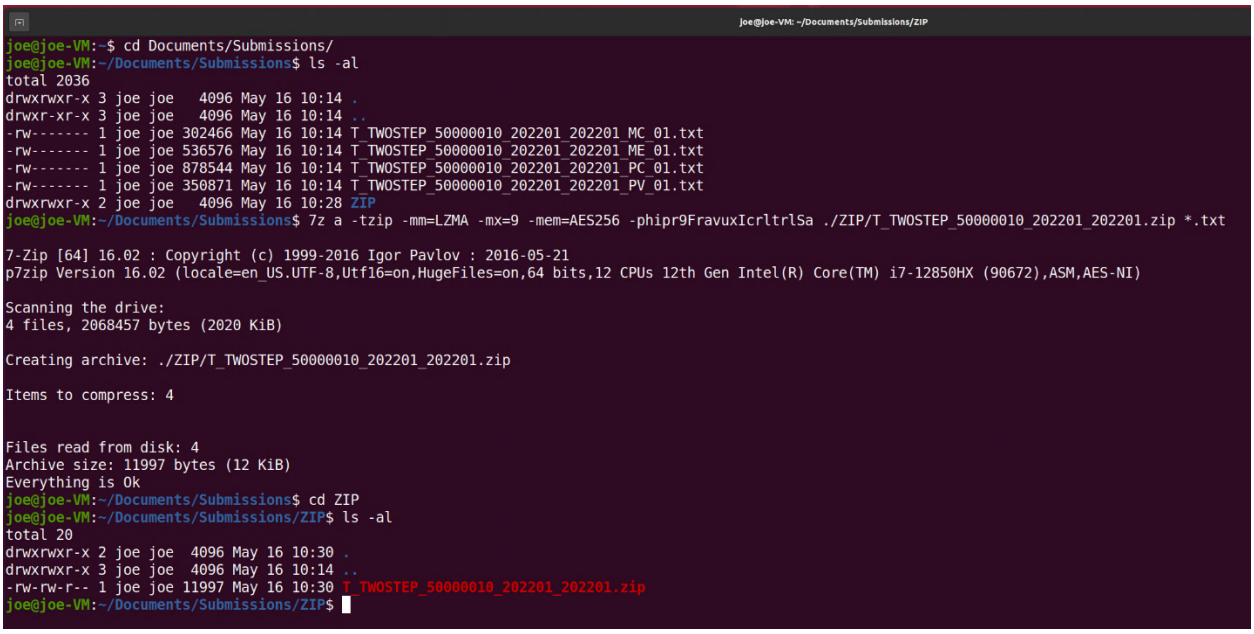
Then the following command can be used to create the zip file package (this assumes that the 64-bit version of 7-Zip was installed):

```
"C:/Program Files/7-Zip/7z.exe" a -tzip -mem=AES256 -m0=lzma -mx=9 -phipr9FravuxlcrltrlSa T_TWOSTEP_50000010_202201_202201.zip *.txt
```

- The executable must 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 like the scenario described above in the Windows example.

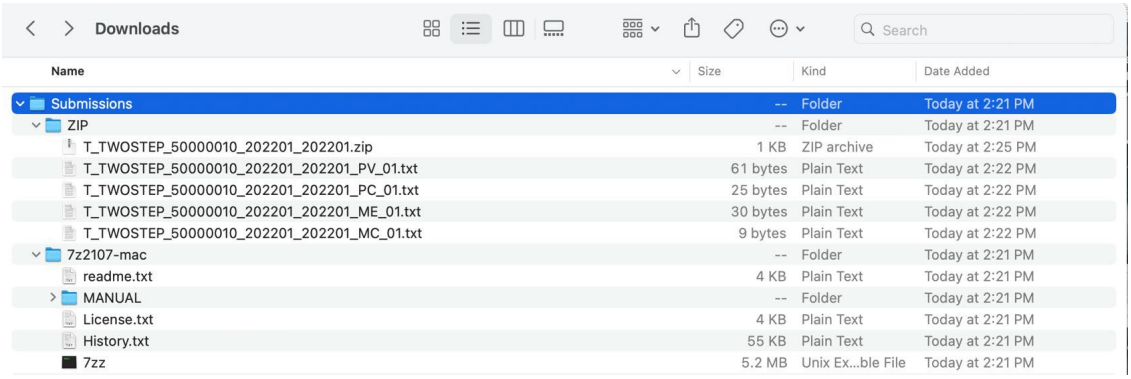


The raw data is in the ~/Documents/Submissions directory in the user's home directory. There is a ZIP sub-folder in which the submission package will be created. The command used to create the zip file package is:

```
7z a -tzip -mm=LZMA -mx=9 -mem=AES256 -phipr9FravuxIcrltrlSa
./ZIP/T_TWOSTEP_50000010_202201_202201.zip *.txt
```

- -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 Submissions 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 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 -phipr9FravuxIcrItrISa
./ZIP/T_TWOSTEP_50000010_202201_202201.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

7.0. 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.

7.1. Secure File Transfer

There are a few 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 the well-known and tested method of SFTP for securely transferring files over the internet.

Before continuing, please note that the submission of files using SFTP requires the input of your TACC MFA code. This impedes any ability to automate the process. If your organization would like to automate submissions, please submit a ticket titled 'MFA Exception' in the TX-APCD submitter portal (https://txapcd.org) under the 'Help' dropdown menu.

7.1.1. Command Line Method

Secure File Transfer Protocol (SFTP) is the command line tool that can be used to transfer files securely over the internet. It is available on Linux, MacOS, and Windows (10+) systems. Several steps are required for a successful file transfer. First, a connection must be established:

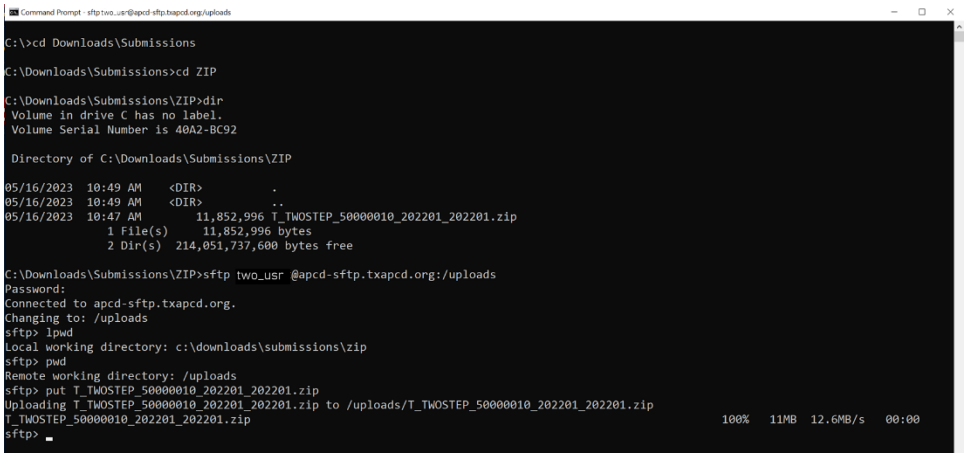
sftp [user]@[host]:[target path]

For example, the following command would start an SFTP session on the TX-APCD SFTP server for user two_usr in the uploads directory.

sftp two_usr@apcd-sftp.txapcd.org:/uploads

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 4.2.

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 SFTP server. 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 SFTP server.



7.1.2. Graphical User Interface Method

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 installation 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.

Linux – use the sha512sum command. For example,

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

MacOS – use the shasum command. For example,

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

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.

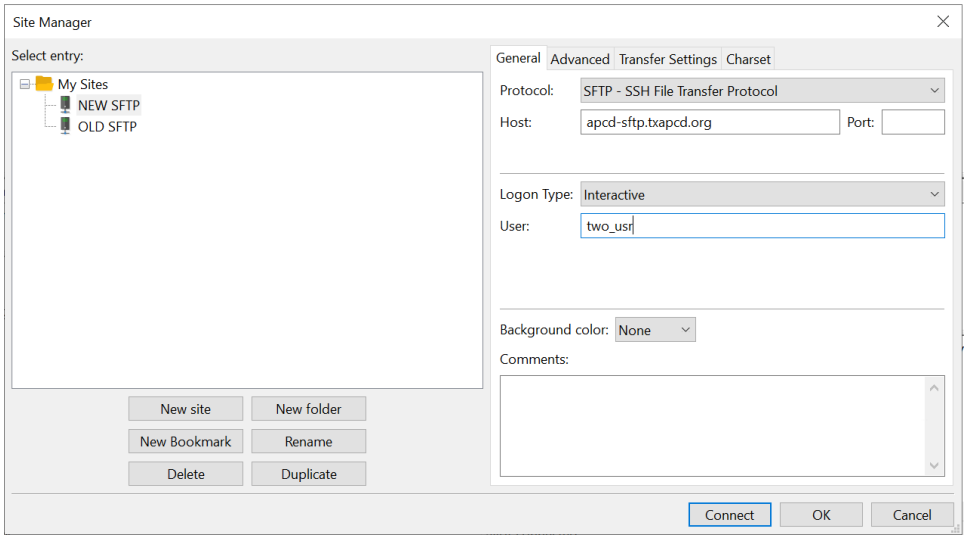
Installing FileZilla

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.

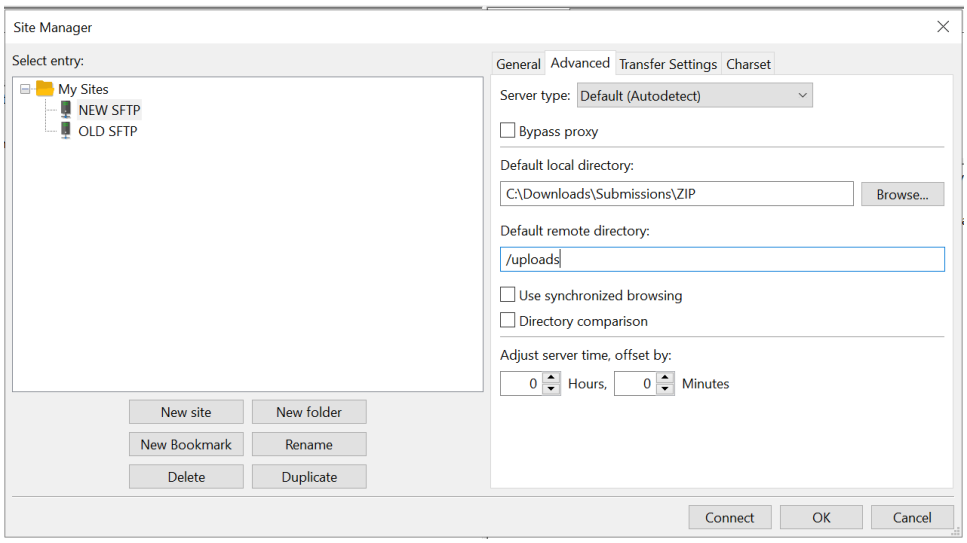
Executing a file transfer using FileZilla

The following series of steps can be used with FileZilla to transfer a file to the TX-APCD.

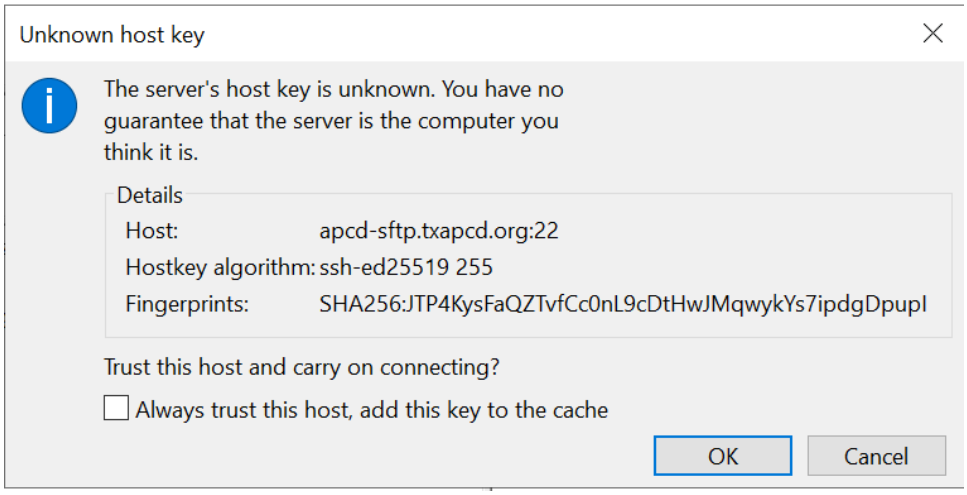
1. Configure the application – start by opening the Site Manager to create a new site. On the General tab, choose ***SFTP*** from the list, and enter ***apcd-sftp.txapcd.org*** as the host. The logon type must be set to ***Interactive***. This is because MFA is required to connect (see section 6.1). 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.

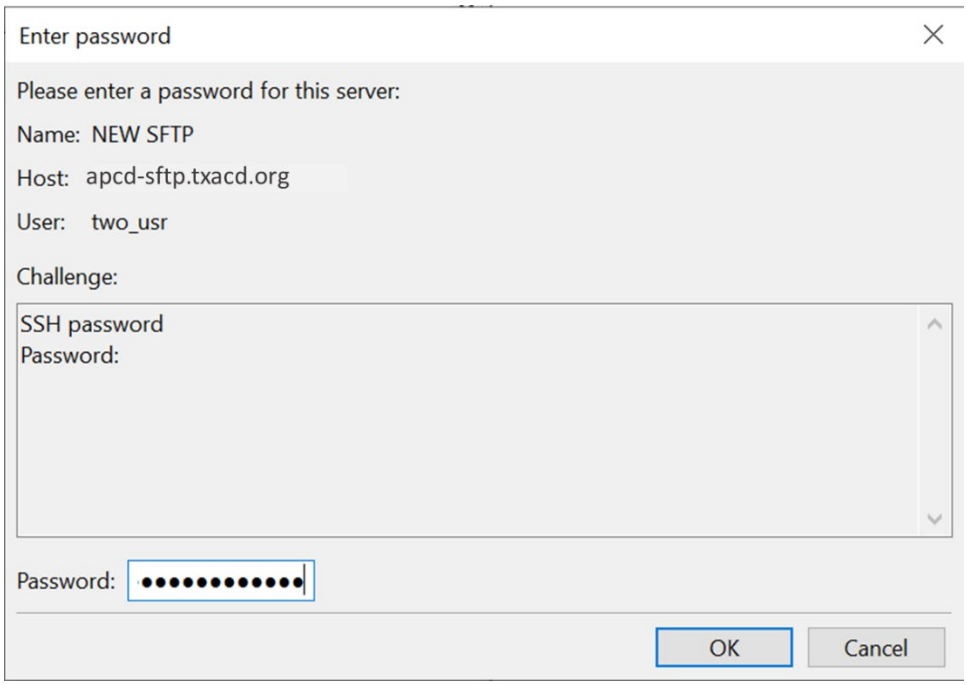


2. Connect to the SFTP site – this is done simply by clicking the "Connect" button. If this is the first time you are connecting to the site, and it has not yet been added as a known and trusted site to the list of local hosts, you will see the following dialog.

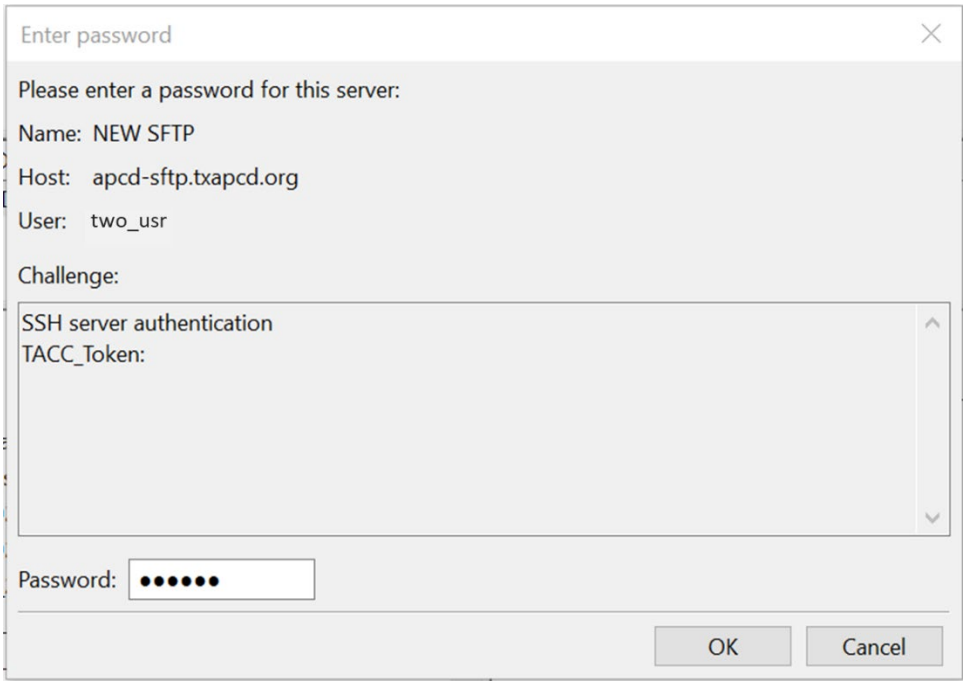


You can choose to trust the remote host and click the "OK" button. You will be prompted each time you connect until/unless you choose to trust the remote host.

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.

7.1.3. Confirming File Transfer Success

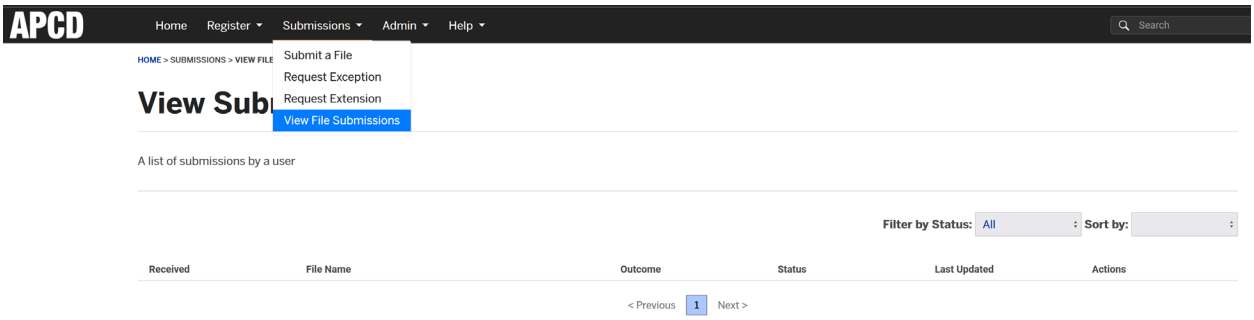
In all the file transfer examples described in this section of the guide, there are three ways to confirm that your file has been transferred successfully:

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 the ZIP file name, time of transfer, and the file's size.

3. All file submission activities will be tracked in the submitter administrative portal. The status of a submission will be visible in the submitter portal within minutes of the submission being received. Follow the Submissions -> View File Submissions menu option.



7.2. 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).

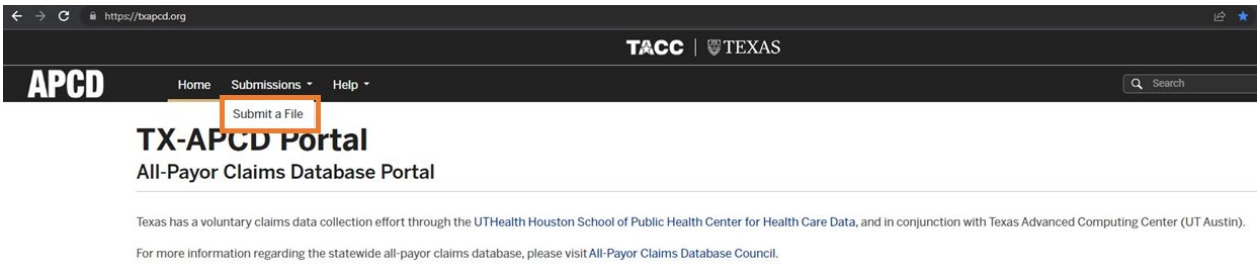
7.2.1. Login to the Submitter Portal

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.

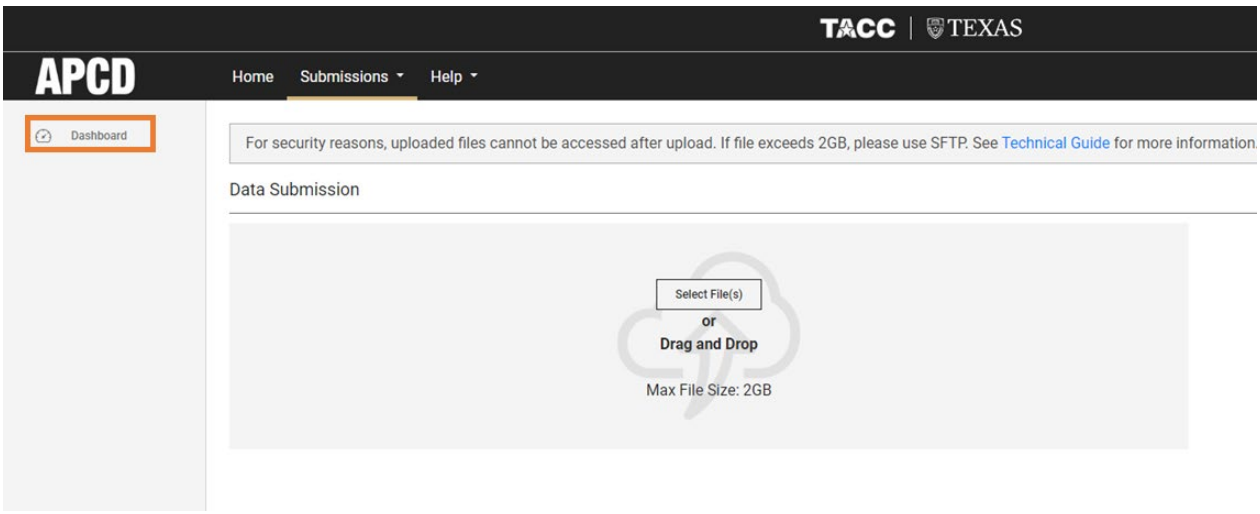
After logging in, you will be on the portal's home page from which you can access all functionality using the available menus. Your access level to functionality in the portal is based on your role's privileges.

7.2.2. 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.



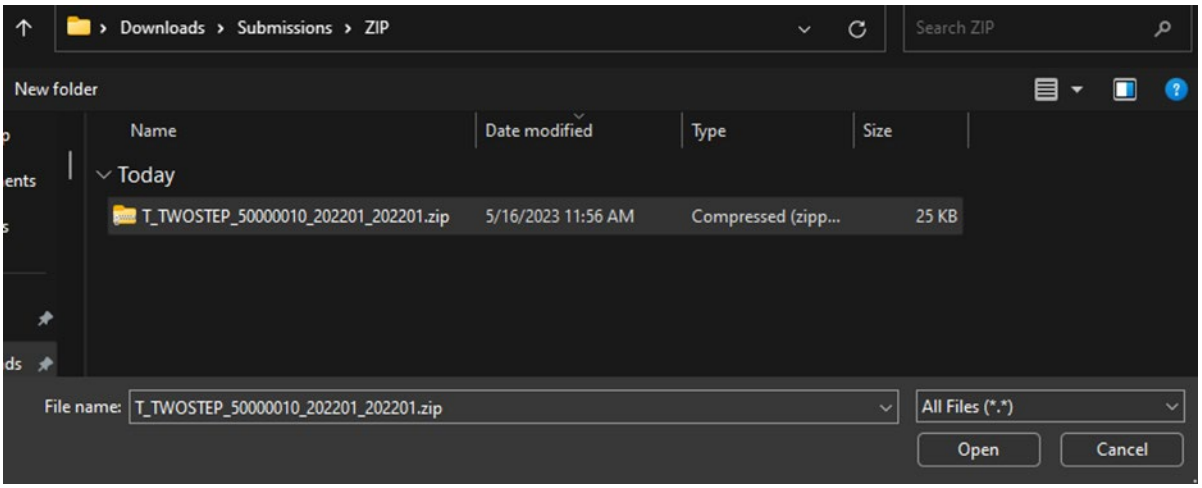
Alternatively, start from the Data Submission item in the menu panel on the left side of the page.



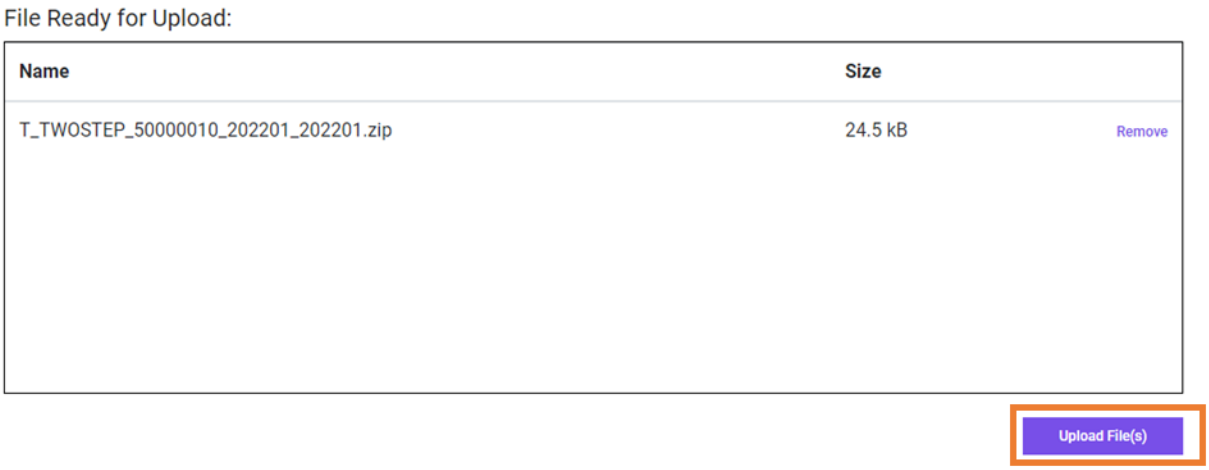
In either case, you will be prompted to select the file you want to upload, or to Drag and Drop the file on to the panel on the right side of the page. You can upload one or multiple files at a time.

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.

7.2.3. 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 7.1.3 also apply to secure web transfer.

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

APPENDIX B – Using GPG Encryption

By default, a symmetric key encryption scheme is used for the encryption of file packages to be submitted to the APCD. This means that the key used to encrypt the package is the key required to decrypt the package. In some cases, a submitter for various reasons might need to use an asymmetric encryption scheme in which a public key is used to encrypt the file, and a separate private key is used to decrypt it. This appendix describes the TX-APCD support for Gnu Privacy Guard (GPG) encryption.

STEP 1 – Submit a Request to Use Asymmetric Encryption

To start the process, the submitter should create a ticket titled "Request to use GPG Encryption." In the ticket, please specify your submitter code and each payor code for which asymmetric encryption will be used. It is preferred for all payor codes associated with a submitter code to use the same encryption scheme (either the default symmetric scheme or the GPG asymmetric scheme).

STEP 2 – Receive Public Key(s)

The TX-APCD support team will generate an asymmetric key pair for each payor code. The key pairs will be loaded into the key repository accessible to the file processing servers. The public keys will be sent to the submitter to be used in the encryption of file packages for submission.

STEP 3 – Use Public Key(s) to Encrypt Files

When encrypting a file package, there are several supported patterns. Since Gnu Private Guard (GPG) and Pretty Good Privacy (PGP) are compatible schemes, both are supported. Files must be in a "package" format when encrypting. For example, a ZIP file package (or a TAR file package) could be created in the process of encrypting a set of text data files. The two patterns that have been used by submitters and are supported by the TX-APCD are zip->pgp and tar->gpg. The symmetric encryption key that was assigned at registration should be used as a passphrase in the encryption process. This

adds another layer of protection for your data. For example, if a tool like Kleopatra is being used to encrypt the files, the “Encrypt with password” should be checked. It is important to note that the TX-APCD is expecting an encrypted file package, so the files should NOT be encrypted separately. If you have specific needs not described in this section, please explain those needs in the ticket you create to request asymmetric encryption. The TX-APCD will do its best to accommodate those needs.

STEP 4 – How the Encrypted Files Get Processed

When the TX-APCD receives a zip.pgp or a tar.gpg package, the first thing that happens is a check for a valid private key in the key repository and a valid symmetric key associated with the relevant payor code. With these two pieces of data, the file is decrypted and repackaged as a standard symmetrically encrypted ZIP file. The repackaged ZIP file is then processed as per normal, generating the appropriate RECEIPT and VALIDATION notifications as the file package gets processed. The reason for repackaging the files is to simplify the management of the thousands of file packages that the TX-APCD expects to receive over the years.

APPENDIX C – Requesting an MFA Exception

For submitters who have an automated process for submitting files to the TX-APCD, multifactor authentication becomes a problem. In such cases an exception can be requested by creating a ticket titled "MFA Exception Request". If granted, a separate "service account" will be created for the submitter (different from the original TACC account). This service account will be associated with an authentication key pair which is what allows for the relaxation of the MFA requirement.

The ticket should include the following information:

(a) A description of how the process is to be automated (ex. which tool is being used?)
(b) The IP address(es) from which submissions will be made (so that the TACC team can whitelist these addresses)
(c) The existing TACC account which will be responsible for the MFA exception.
(d) The preferred name for the service account to be created. The TACC team may override this preference to avoid clashes with existing names, or for other internal reasons.
(e) The public key from a key pair generated by the submitter for the purpose of authentication (can be attached as a file to the ticket). The public key should be in OpenSSH format (often a .pub file). If the key pair has been created with a tool like PuTTygen (by default a .ppk file), it will need to be converted to SSH2 format. This conversion can be done using PuTTygen.

The TACC team will review the request and may ask further questions for clarification. If the request is granted, the submitter will be provided with the new service account along with instructions on how to submit their files. If issues as encountered with automation, please consult the FAQ section of the TX-APCD website for information or create a ticket requesting assistance with the issue.