New York State Department of Health All Payer Database

Encounter Intake System (EIS)

Standard Companion Guide Trading Partner Information

Instructions Related to the Exchange of Electronic Data Interchange (EDI) with the EIS.

Based on X12 Implementation Guides, Version 5010 and the NCPDP Implementation Guide, Version 4.2.

Trading Partner Information Version Number: 1.5

Table of Contents

Table of Figures

1 Introduction

1.1 Purpose

This document is intended to provide information needed by trading partners to exchange Electronic Data Interchange (EDI) data with the Encounter Intake System (EIS). This includes information about registration, testing, support, and specific information about control record setup.

1.2 Scope

This EIS Trading Partner Information Companion Guide is intended as a resource to assist issuers, their third party administrators, and all other trading partners of the All Payer Database (APD) EIS in successfully conducting EDI of Post Adjudicated Claims Data Reporting (PACDR) transactions. This document provides instructions for enrolling as an EIS Trading Partner, obtaining technical assistance, initiating and maintaining connectivity, sending and receiving test files, and other related information. This document does not provide detailed data specifications, which are published separately by the industry committees responsible for their creation and maintenance.

1.3 Overview

This guide provides communications-related information a Trading Partner needs to enroll as a Trading Partner, obtain support, format the X12 Interchange Control Header (ISA) and Functional Group Header (GS) envelopes, the NCPDP Header and Trailer information, and exchange test transactions with the EIS.

1.4 Security and Compliance Standards and Requirements

All submissions will be conducted using the safeguard controls and processes provided as part of the Trading Partner Agreement and the trading partner registration process and will be in accordance with all appropriate data privacy standards as defined by the Affordable Care Act (ACA), Health Information Portability & Accountability Act (HIPAA), Centers for Medicare and Medicaid Services (CMS) and the National Institute of Standards and Technology (NIST).

1.5 References

Encounter related Frequently Asked Questions (FAQs), Crosswalks, and resources such as a complete set of EIS Companion Guides are obtained from either NYSOH Plan Management or the OHIP Bureau of Managed Care and Fiscal Oversight.

For NYSOH Qualified Health Plans and Essential Plans, the NYSOH Listserv is maintained by the DOH Plan Management Department of the NYSOH (hereafter referred to as “NYSOH Plan Management”). Please contact NYSOH Plan Management at 518-486-9102 or email nysoh_issuer_support@health.ny.gov to be added to the Listserv.

For Medicaid Managed Care Plans the MEDS Listserv is maintained by the Bureau of Managed Care and Fiscal Oversight. Please contact the Bureau at (518) 474-5050 or email omcmeds@health.ny.gov to be added to the Listserv.

The Encounter related documentation is available on the NYSOH Issuer Portal. New requests for access to the Issuer Portal should be sent to NYSOH Plan Management (nyhxpm@health.ny.gov) and the NYS APD team (nysapd@health.ny.gov).

2 Getting Started

2.1 Working Together

EIS - Encounters support services for the X12 837 and NCPDP PACDR transactions can be requested through the following e-mail address:

NYS-DOH-APD-ISSUER-SUPPORT@csra.com

2.2 Trading Partner Registration

2.2.1 EIS Enrollment

EIS Enrollment

An EDI Trading Partner is any entity (Issuer, Clearinghouses, Billing Service, Third Party Administrator, Software Vendor, Financial Institution, etc.) that transmits electronic data to or receives electronic data from another entity. The EIS requires any Trading Partner that wishes to exchange electronic data to be enrolled and have a Trading Partner Profile. Entities meeting the definition of a Trading Partner may enroll with the EIS by completing a Trading Partner EDI Registration form. Trading Partners currently exchanging 834 transactions with the EIS have already established Trading Partner Profiles. For existing Trading Partners, no additional enrollment process is required for encounter submission.

Qualified Health Plan and Essential Plan Issuers may request EDI Registration forms for new Trading Partners by contacting NYSOH Plan Management at 518-486-9102 or via email at nysoh_issuer_support@health.ny.gov

Medicaid Managed Care Plans can obtain Trading Partner and EDI Registration forms by contacting the OHIP Bureau of Managed Care and Fiscal Oversight at (518) 474-5050 or by email at omcmeds@health.ny.gov

Note: Issuers that choose to have a Third Party Administrator submit on their behalf, must initiate and coordinate the enrollment of said Third Party Administrator with NYSOH Plan Management (QHP and Essential Plan Issuers) or the Bureau of Managed Care and Fiscal Oversight (Medicaid Managed Care Plans).

EDI Trading Partner Agreement

An EDI Trading Partner Agreement is a contract between parties that have chosen to become electronic business partners for the EIS. The EDI Trading Partner Agreement stipulates the general terms and conditions under which the partners agree to exchange information electronically. The document defines participant roles, communication, and security requirements.

All Trading Partners must have a Trading Partner Agreement on file before proceeding with EDI.

Once the agreement is processed, a Trading Partner Identification Number (TPIN) is assigned. The entity will be notified via secure email from the EIS Encounter Support Services for Issuers. The Pre-Production (Issuer Test Environment) and Production SFTP systems, Internet Protocol (IP), Port numbers, User ID and Password will be returned to the Issuer on the EDI Registration response document.

Note: Any time a company enrolled as a Trading Partner with the EIS changes their tax identification (ID), the company is treated as a new company, thereby requiring new testing, etc.

2.3 Connectivity

Connectivity / Communications

The EIS ensures the security and privacy of Protected Health Information (PHI) data being transmitted by its Trading Partners over the internet. Trading Partners will connect to the EIS via Secure File Transfer Protocol (SFTP) for batch processing.

Access Methods

Connection is made to the SFTP environment via two (2) IP addresses for the EIS, one for the pre-production (Test) environment and one for the production environment. The EIS Host Names, IP addresses and Port Numbers for each environment will be sent to the Issuer when the EDI Registration process is completed.

Notes:

- Test files sent to the wrong IP address will **NOT** be processed.
- Files submitted to the production environment before the Issuer / Third Party Administrator is approved for submission will not be processed.

Guidelines for using SFTP

For each Trading Partner, the EIS will set up an SFTP mailbox with Inbox and Outbox folders in the pre-production (Test) and the production environments. The EIS will pick up inbound files from the Inbox. The EIS batch process runs multiple times per day and will place all EIS outbound files into the Outbox. All EIS inbound files will be removed from the Inbox as files are processed. EIS response files will be returned to the SFTP Outbox.

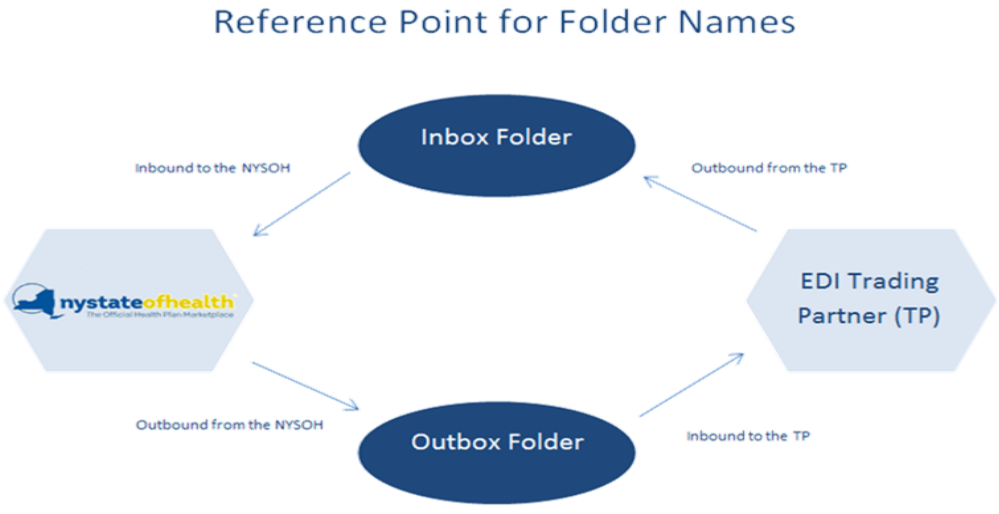


Figure 1: EIS Process Flow

2.4 Supported Transactions

The EIS supports the approved versions of the X12 and NCPDP Post Adjudicated Claims Data Reporting (PACDR) electronic health care transactions. Listed below are the supported inbound and outbound transactions.

Inbound transactions:

- PACDR (837): Professional version 005010X298
- PACDR (837): Institutional version 005010X299
- PACDR (837): Dental version 005010X300
- Post Adjudicated Claim Standard (NCPDP) version 4.2

X12 Outbound transactions:

- RJ File Rejection (when file envelope is deemed unreadable)
- File Level Handshake (TA1)
- Implementation Acknowledgement for Health Care Insurance (999) ASC X12C 005010X231A1
- Health Care Claim Acknowledgement (277CA) ASC X12N 00510X214

NCPDP Outbound transactions:

- Rx Healthcare File Acknowledgement (RxFA)
- Rx Healthcare Transaction Acknowledgement (RxTA)
- Rx Healthcare Claim Acknowledgement (RxCA)

3 Testing

All new EIS EDI Trading Partner accounts are initially set up in the Issuer Testing Environment (ITE) which is designed to establish SFTP credentials and confirm that service is configured to exchange EDI transactions with the EIS. In this phase of testing, the Trading Partner downloads and uploads a limited number of initial test files provided by the EIS via Secure File Transfer Protocol (SFTP). Once SFTP credentials and service have been confirmed, Trading Partners may progress to Encounter Data Testing. Issuers will be working with the EIS Customer Care team and the APD throughout testing.

Please note: Under no circumstance can production data be submitted to the testing environment.

Encounter Testing

The APD will utilize a multi-phased approach for Issuer Testing of the EIS.

Phase 1: Network Connectivity Testing

Test Objectives Include:

- Confirm Issuers have SFTP credentials and service is configured to submit files to the EIS.
- Determine the Issuer is capable of submitting files with the proper naming convention and retrieving responses via SFTP.

Phase 2: Pre-Production Testing in the Issuer Test Environment

Test Objectives Include:

- To offer Issuers the ability to test all transactions types from end-to-end.
- To verify and report back to the Issuer on data structure and content to the same degree of stringency as the production environment.

After successful completion of Phase 1 & 2 testing, a Trading Partner will be approved to submit to production. Files sent to production prior to approval will not be processed.

Testing Instructions

Phase 1: Network Connectivity Testing

- Trading Partners receive Network Connectivity instructions from the EIS. If necessary, a connectivity test will be scheduled with Data Security for 10pm on a designated business day.
- Trading Partner must add their HIOS or Third Party Administrator ID to the ISA and GS Segments:
  - ✓ For Issuers submitting encounter data on their own behalf, ISA06 and GS02 will contain the Issuer's HIOS ID.
  - ✓ For Third Party Administrators submitting on behalf of an Issuer, ISA06 must contain the Third Party Administrator's ID and GS02 must contain the Issuer's HIOS ID.
- ISA14 must have a value of '1' to indicate a submission response is requested.

- Trading Partner must properly name the inbound file according to the Naming Convention outlined in Section 3.1.5.
- Each Trading Partner will upload the PACDR 837P (Professional) transaction file to their Pre-production (Test) Inbox via SFTP.
- After the EIS receives the PACDR 837P (Professional) transaction file via SFTP, the system will check the file's envelope and a TA1 or RJ response will be generated within 24 hours.
- Trading Partners should promptly retrieve their response files. The EIS will archive response files that have been picked up by a Trading Partner.
- At the successful conclusion of this test, the Trading Partner is verified to have successfully completed Connectivity testing and may proceed to Phase 2 Pre-production Testing.

Phase 2: Pre-Production Testing

- For testing purposes, the NYS APD team will supply each Issuer with a Member Data Test file which contains PHI-free member information for testing purposes. The member data file contains member demographic information that is free of PHI. Issuers **must** use the supplied member test data when testing transactions with the EIS. Failure to use the member test data will result in the file being quarantined and notification to our Security and Compliance Officer as well as the Issuer.
- Each Trading Partner will upload a PACDR transaction file to their test Inbox via SFTP.
- After the EIS receives the PACDR transaction file via SFTP, the system will process the file and return the appropriate responses. See section 3.1.7 for file processing stages and responses generated at each stage of file validation.

Guidelines for successful testing:

- ***Use only the member test data supplied by the APD team.***
- Begin testing with a single transaction type.
- Submit a very small file initially, which contains only a few encounters, and move to large files once successful submission is achieved.
- Retrieve and reconcile response files promptly.

3.1 Testing Requirements

The EIS Issuer Testing Environment (ITE) enables Trading Partners to conduct end-to-end testing.

In order to utilize the EIS test environment the following components are required:

- An active EIS Account and User ID with a registered Issuer/Third Party Administrator IP address.
- An active Trading Partner Agreement on file with NYSOH Plan Management or the Bureau of Managed Care and Fiscal Oversight

3.1.1 X12 and NCPDP Transaction Versions

The EIS Pre-Production (Test) and Production environments accept and process only:

- ASC X12 PACDR v 5010
- NCPDP v 4.2

3.1.2 Test Limitations

The ITE system transaction file size limits set for inbound files differ from the EIS production environment's limits.

- Submitters are limited to sending two transmissions (two physical files) to the ITE per 24-hour period.
- All file submissions are limited to 50 records or claim transactions. The specific data items counted in each transaction are as follows:

Transaction	Loop-Segment	Counting Instruction
837 (All)	2300-CLM	Each CLM Segment constitutes a claim
NCPDP	N/A	Each Post Adjudication History Detail Record (Record Type = DE) constitutes a claim. ITE limits the Trailer Record Total Record Count field to not exceed 50

3.1.3 Test Availability and Submission Cutoff Times

The EIS Pre-production (Test) environment will be available continuously for submitting test transactions and receiving associated responses.

3.1.4 Submitting Files to the EIS

Before submitting files to the EIS, the Trading Partner must:

For X12 transactions:

- Verify the Trading Partner ID in data elements ISA06 (Interchange Sender ID) and GS02 (Application Sender's Code) is the Issuers' HIOS ID and / or Third Party Administrator (TPA) ID.
  - ✓ For Issuer submissions, ISA06 Interchange Sender ID and GS02 Application Sender's Code must be the Issuer's HIOS ID and must match the User ID in the file name
  - ✓ For Third Party Administrator submissions, ISA06 Interchange Sender ID must contain the TPA ID, GS02 Application Sender's Code must contain the Issuer's HIOS ID and the file name User ID node must contain the TPA ID + the Issuer's HIOS ID
- Verify the value in ISA08 Interchange Receiver ID and GS03 Application Receiver's Code is "NYSOH-ENC".
- Verify there is only one ISA/IEA per file.
- Verify there is only one Functional group (GS/GE) for each envelope (ISA/IEA).
- Verify the ISA13 Interchange Control Number is unique for all of an Issuer's submissions.
- To receive a submission response, verify the ISA14 Acknowledgement Requested is populated with a value of '1'.

For NCPDP transactions:

- Ensure the Post Adjudicated History File format is being used (NOT the Post Adjudication Utilization File format).
- Verify there is one Header Record (PA), one Trailer Record (PT), and at least one Detail Record (DE).
- Verify the 806-5C Batch Number is unique for all of an Issuer's submissions.
- Verify the 880-K7 Receiver ID is equal to "NYSOH-ENC".
- For Issuer Submissions, verify the Issuer's HIOS ID is entered in field 879 (Sending Entity Identifier).
- For Third Party Administrator (TPA) submissions, verify the TPA ID + the Issuer's HIOS ID is entered in field 879 (Sending Entity Identifier).
- Verify the UserID in the file name matches the Sending Entity Identifier.
- Verify record/line terminator is a Line Feed (LF).

For all transactions:

- Limit the file size to 50 claims/records for test.
- Apply a unique file name with no spaces or special characters in accordance with the file naming conventions listed below (see section 3.1.5).

Test transactions are directed to the EIS Issuer Test Environment by:

- Uploading the test file to the inbox associated with Test IP address (ending in .13) assigned by the EIS during initial enrollment.
- Setting the appropriate indicator on the inbound file.
  - ✓ **ASC X12 Transactions:** For all ASC X12 Transactions, the Usage Indicator (Data Element ISA15) should be set to a value of "T". Example:

    ISA*00* *00* *ZZ*HIOS# *ZZ*NYSOH-ENC *010806*1200*^*00501*000000008*1*__**T**__*:~
  - ✓ **NCPDP Transactions (Batch Only):**

    The Batch Header File Type (702-MC) should be set to a value of "T".

3.1.5 Inbound File Naming Convention

File Naming Convention for inbound files exchanged with the Encounter Intake System is:

(Tran Category). (UserID). (Transaction)(Program Suffix).(Frequency).(Date Time).(SEQNO).(DAT)

Values for each node

Tran Category

TR – Transaction

UserID

SFTP User Id assigned by the EIS

The correct format for an Issuer ID is NYE followed by the five digit HIOS number (example: NYE12345).

Transaction

837I – Institutional 837
837P – Professional 837
837D – Dental 837
PDP – NCPDP pharmacy

Program Suffix

Q – QHP
M – Medicaid / CHP
E – Essential Plan

Frequency - Default Weekly

D – Daily
W – Weekly
B – Bi-weekly
M – Monthly

Date Time

12 digit date and time stamp (24-hour time, in the format YYMMDDHHMMSS)

Sequence Number

A sequence number to uniquely identify the file within the timestamp.

File Extension as .DAT

Example:

Inbound Transaction for an 837P Submission:

Transaction Type	Inbound File Name
Professional 837 from a QHP Issuer	TR.NYE12345.837PQ.W.130430135202.001.DAT
Professional 837 from a Medicaid/CHP Issuer	TR.NYE12345.837PM.W.130430135202.001.DAT

Transaction Type	Inbound File Name
Professional 837 from an Essential Plan Issuer	TR.NYE12345.837PE.W.130430135202.001.DAT

Inbound File Naming Conventions for EIS - Third Party Administrators Only

While the EIS is leveraging the existing naming conventions as utilized in the 834 EDI transactions for standard Issuer submitted files, the Third Party Administrator submission naming convention uses a prefix modification in order to provide the capability to manage the submission by proxy. The Third Party Administrator File naming convention will produce a direct link of Third Party Administrator, Issuer and transaction type (i.e., professional, institutional, dental or NCPDP) that will allow the processing system to validate the Third Party Administrator relationship to the Issuer as well as the eligibility to submit the specific Encounter data transaction type.

The Third Party Administrator ID will always be combined with the Issuer ID in all submissions to provide clear identification of TPA and Issuer relationship.

The User ID is a combination of Third Party Administrator ID + ISSUER ID

(Tran Category).(UserID).(Transaction)(ProgramSuffix).(Frequency).(DateTime).(SEQNO).(XXX)

Example of a Professional 837 submitted by a Third Party Administrator:

TR.**T0901054546**.837PQ.W.130430135202.001.DAT

Note: The format of a Third Party Administrator ID is 6 characters beginning with T09.

3.1.6 Outbound File Naming Convention

All outbound files sent to Issuers for download are created with the following naming convention:

(Tran Category).(UserID).(Transaction)(Program Suffix).(Frequency).(DateTime).(SEQNO).(DAT)

Values for each node

Tran Category

RJ – Reject File
IA – TA1 X12 or RxFA (Interchange Acknowledgment)
FA – Interchange Acknowledgment (999 or RxTA Report)
HN – Healthcare Claim Acknowledgment (277CA or RxCA)

UserID

NYHBE

Transaction

837I – Institutional 837
837P – Professional 837
837D – Dental 837
PDP – NCPDP pharmacy

Program Suffix

Q – QHP
M – Medicaid / CHP
E – Essential Plan

Frequency - Default Weekly

D – Daily
W – Weekly
B – Bi-weekly
M – Monthly

Date Time

12 digit date and time stamp (24-hour time, in the format YYMMDDHHMMSS)

Sequence Number

A sequence number to uniquely identify the file within the timestamp.

File Extension as .DAT

Examples:

Response Transactions for a QHP 837P Submission:

Transaction Type	Outbound File Name
RJ File Rejection	RJ.NYHBE.837PQ.W.130430135202.001.DAT
TA1 Response	IA.NYHBE.837PQ.W.130430135202.001.DAT
999 Acknowledgments	FA.NYHBE.837PQ.W.130430135202.001.DAT
277CA Acknowledgment	HN.NYHBE.837PQ.W.130430135202.001.DAT

Response Transactions for a MMC/CHP 837P Submission:

Transaction Type	Outbound File Name
RJ File Rejection	RJ.NYHBE.837PM.W.130430135202.001.DAT
TA1 Response	IA.NYHBE.837PM.W.130430135202.001.DAT
999 Acknowledgments	FA.NYHBE.837PM.W.130430135202.001.DAT
277CA Acknowledgment	HN.NYHBE.837PM.W.130430135202.001.DAT

Response Transactions for an Essential Plan 837P Submission:

Transaction Type	Outbound File Name
RJ File Rejection	RJ.NYHBE.837PE.W.130430135202.001.DAT
TA1 Response	IA.NYHBE.837PE.W.130430135202.001.DAT
999 Acknowledgments	FA.NYHBE.837PE.W.130430135202.001.DAT
277CA Acknowledgment	HN.NYHBE.837PE.W.130430135202.001.DAT

Response Transactions for a QHP NCPDP Submission:

Transaction Type	Outbound File Name
RxFA Acknowledgment	IA.NYHBE.PDPQ.W.130430135202.001.DAT
RxTA Acknowledgment	FA.NYHBE.PDPQ.W.130430135202.001.DAT
RxCA Acknowledgment	HN.NYHBE.PDPQ.W.130430135202.001.DAT

Response Transactions for a MMC / CHP NCPDP Submission:

Transaction Type	Outbound File Name
RxFA Acknowledgment	IA.NYHBE.PDPM.W.130430135202.001.DAT
RxTA Acknowledgment	FA.NYHBE.PDPM.W.130430135202.001.DAT
RxCA Acknowledgment	HN.NYHBE.PDPM.W.130430135202.001.DAT

Response Transactions for an Essential Plan NCPDP Submission:

Transaction Type	Outbound File Name
RxFA Acknowledgment	IA.NYHBE.PDPE.W.130430135202.001.DAT
RxTA Acknowledgment	FA.NYHBE.PDPE.W.130430135202.001.DAT
RxCA Acknowledgment	HN.NYHBE.PDPE.W.130430135202.001.DAT

Note: The DateTime and sequence number on outbound files will match the DateTime and sequence number submitted by the Issuer on the inbound file to facilitate reconciliation of responses from the EIS.

3.1.7 File Processing

The Encounter File Submission is a process that manages the files submitted by Issuers.

Each Issuer's File will be picked up and the envelope sections will be verified (ISA/GS for X12 and Header/Trailer for NCPDP). To avoid re-submissions from the Issuer, the system will immediately respond to the inbound file with a file acknowledgement (either a TA1 for X12 or an RxFA for NCPDP) letting them know the Encounter Intake System correctly received their file. The Encounter Intake System will also check for duplicate Interchange Control / Batch Numbers to eliminate any duplicate processing. For X12 transaction files, if the file is unreadable an RJ File will be immediately returned. All readable test and production inbound files will be put into a Staging Folder to be held until the next batch processing cycle.

The validation routine will sort files by the Issuer, date, and sequence number within the file name to ensure originals and adjustment/voids are processed in the correct order. Tier I and Tier II editing will be performed, which encompasses HIPAA Compliance Types 1 through 5 and DOH required edits.

Tier I file level editing includes Compliance Types 1 through 4:

- Type 1 (EDI Standard Integrity Testing) validates the basic syntactical integrity of the EDI submission. Type 1 conducts a test for valid segments, segment order, element attributes (e.g., numeric values in numeric data elements, correct field length), validation of X12 or NCPDP syntax, and compliance with X12 rules.
- Type 2 (HIPAA Implementation Guide Requirement Testing) involves testing for HIPAA Implementation Guide specific syntax requirements, like limits on repeat counts, used and not used qualifiers, codes, elements and segments.
- Type 3 (HIPAA Balance Testing) checks transaction balanced field totals, financial balancing of claims or remittance advice, balancing summary fields etc. Transaction balancing will occur within the Encounter Validation routine. This will ensure the encounter Total Claim Charge balances with the sum of line level payments and claim level adjustments.
- Type 4 (HIPAA Inter-Segment Situation Testing) involves testing of specific inter-segment situations described in the HIPAA implementation guides, such that if A occurs then B must be populated etc.

Tier II encounter level editing includes Compliance Type 5 and DOH required business rules:

- Type 5 (HIPAA external code set testing) involves testing for valid Implementation Guide specific code set values and other code sets adopted as HIPAA standards such as ICD-9-CM or NDC code sets. X12 Submission / Response / Acknowledgement Process
- DOH required business rules are contained in the EIS Companion Guides and Edit Documents

3.1.8 X12 Response Files for each level of validation

RJ File Response: The EIS will generate an RJ File if the envelope is unreadable for X12 PACDR files.

TA1: When an Issuer sends an X12 PACDR file via SFTP, a TA1 will be sent back as a handshake acknowledging the EIS successfully received the transmission. This acknowledgement will indicate whether the file was rejected or accepted for processing in the EIS. If the file is rejected, the appropriate error code will be returned.

If the file is accepted for processing, it will be staged for encounter validation which will be run as the processing schedule permits.

If a Trading Partner does not receive a RJ or TA1 response within 48 hours, they should contact EIS Encounter Support Services for Issuers at **NYS-DOH-APD-ISSUER-SUPPORT@csra.com.**

999: A batch job will process the Issuer's PACDR file. A 999 acknowledgement will be created when at least one Tier I error is found. Tier I edits on X12 transactions will contain all Type 1 through Type 4 HIPAA compliance types.

Any Tier I errors in the file will result in a complete file rejection. The purpose of the 999 Functional Acknowledgement is to report back if the file passed standard level syntax and structure editing Tier I (Type 1 through Type 4) HIPAA compliance checks. Since any file failing Tier I edits will be completely rejected, the 999 response will only contain error information. A 999 will not include accepted transactions.

277CA: The EIS process will check to ensure functional edits are met (external code sets and logical validation). The 277CA will be created with the results of Tier II editing. The status of each claim (accepted or rejected) will be reported on the 277CA using standard X12 codes.

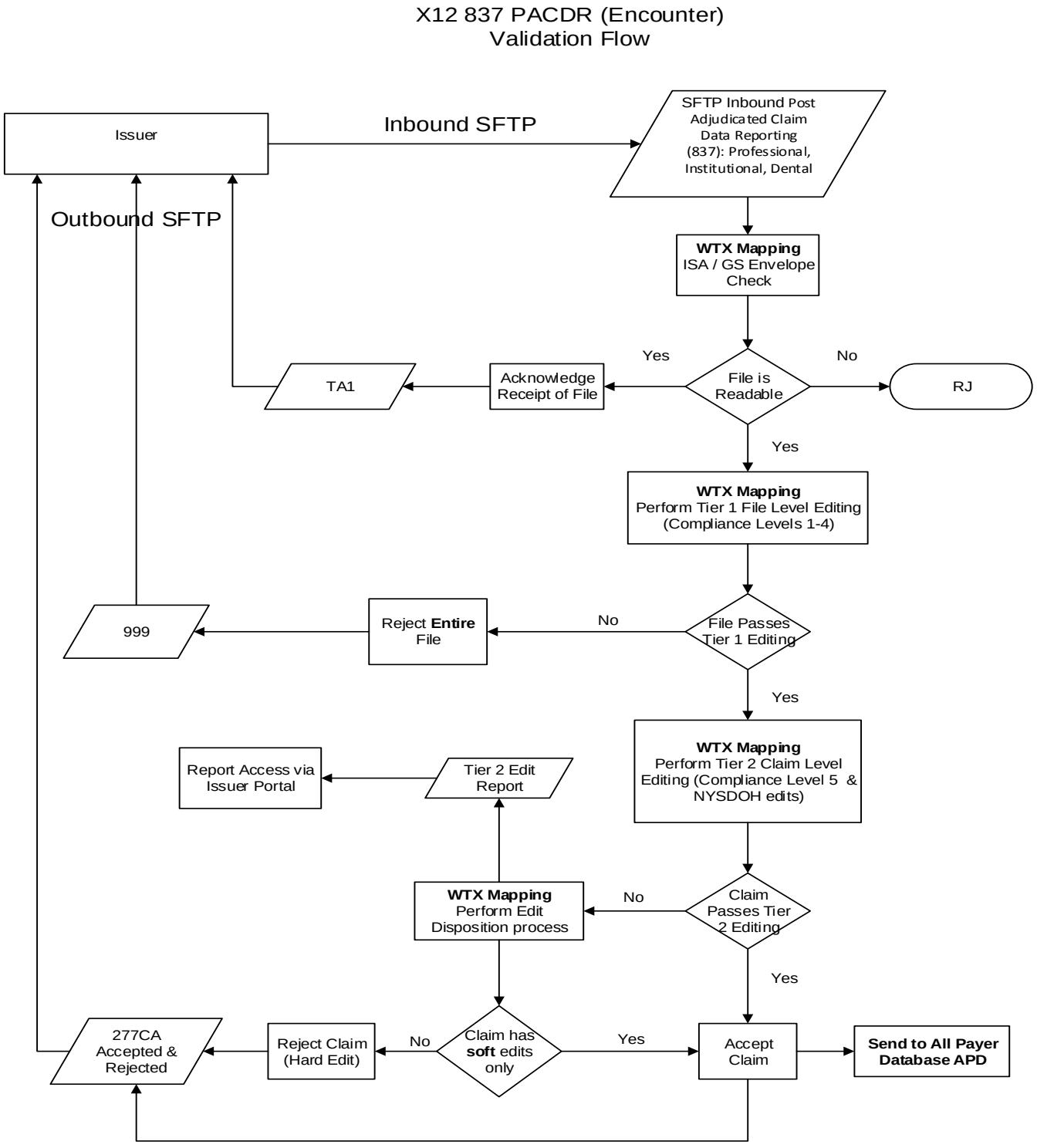


Figure 2: X12 Submission / Acknowledgement / Response Process

3.1.9 NCPDP Response Files for each level of validation

RxFA (File Acknowledgement): The RxFA will be sent back to verify the EIS successfully received the transmission and the file is readable/unreadable. The RxFA will indicate if the file was accepted or rejected. If the file is rejected, the appropriate error codes will be returned.

If the file is accepted, it will be staged for encounter validation which will be run as the processing schedule permits.

RxTA (Transaction Acknowledgement): The purpose of the Rx Transaction Acknowledgement is to report if the file passed standard level syntax and structure editing Tier I (Type 1 through Type 4) HIPAA compliance checks. Since any file failing Tier I edits will be completely rejected, the RxTA response will only contain error information. The RxTA will not include accepted transactions.

RxCA (Claim Acknowledgement): The EIS process will check to ensure functional edits are met (external code sets and logical validation). The RxCA will be created with the results of Tier II editing. Each claim (whether accepted or rejected) will be reported on the RxCA. Multiple rows per claim may be generated on the file for each edit failed by a claim. The edits will be identified using proprietary EIS Encounter System edits. The status (accepted or rejected) of each claim will be reported using proprietary EIS Encounter System codes.

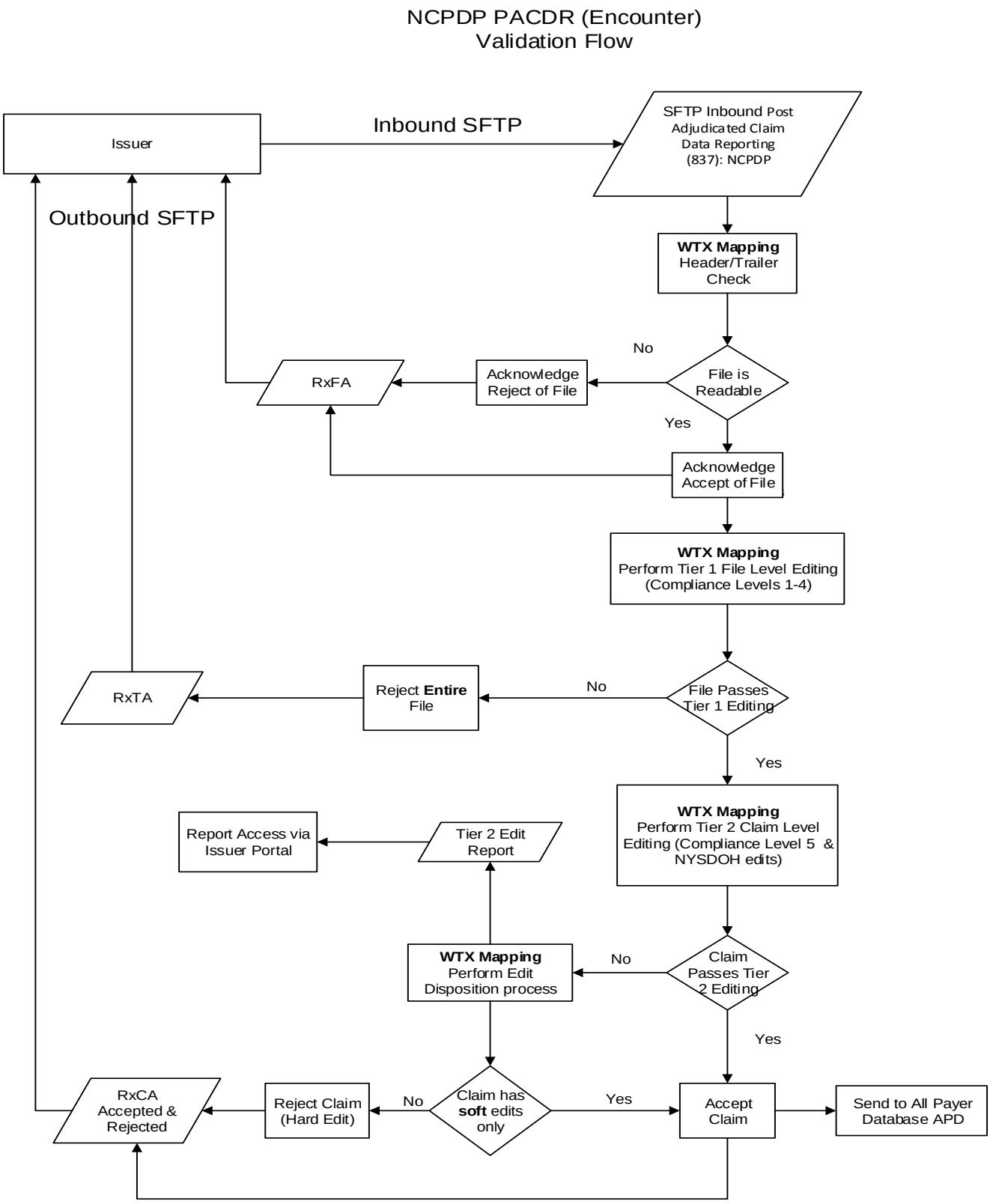


Figure 3: NCPDP Submission / Acknowledgement / Response Process

3.1.10 Information Security Data Release and Validation Management

As a key part of protecting sensitive information coming in and out of the EIS as well as mitigating potential risks, we are providing our partners with established standards and guidelines for sending and receiving data in a way that checks and balances are in place and to ensure the protection of the partners and the EIS. The EIS has established very tight restrictions based on federal requirements, ACA rules, HIPAA Privacy Rules, and NIST 800-53a Rev safeguard standards on our platform for information management and to the extent we use internal processes to validate information received in accordance with appropriate federal guidelines and industry standards for data acceptance and release management.

To exchange health information, two or more organizations will be involved. To secure the exchange of health information, the exchanging organizations and the means of conducting the exchange must have appropriate security and privacy controls.

To ensure that health information is adequately protected, the "non-exchange" portions of the data usage, including collection, storage, modification, and destruction, must also receive security and privacy protections, which may include contingency, configuration management, and other processes and technologies whether direct safeguards or by developing compensating controls to meet minimum safeguard standards.

The function of these processes is to provide a standard set of minimum requirements between the EIS and the Issuer or Third Party Administrator, but not to establish definitive methods for receiving or obtaining data. This means that every Issuer/Third Party Administrator or connecting entity will need to deploy secure services using appropriate solutions, validations and processes that must be identified and selected as part of the data release and acceptance management standards. Having a consistent, standards-based set of processes and validations can benefit future interoperability among our organizations.

This section provides recommended processes and guidelines that Issuers and their Third Party Administrators should consider implementing. These standards apply to all data whether test or production data. The EIS will not accept any production data for the purposes of testing and must meet all requirements outlined as part of the Issuer registration form, addendum and this companion guide.

The data release and validation management for this program offer the following that as Issuers and their Third Party Administrators progress through the maturity curve will continue to be a foundation from which to measure our success relating to data assets. It will:

- Transfer health data using predictable business processes and accommodate necessary ethical and regulatory demands
- Reduce operational friction (Provide "*right-data, right–time*")
- Protect the needs of both data stakeholders
- Build standard, repeatable processes
- Reduce costs and improve efficiency through coordination of efforts (*People, Process, Technology, Regulatory*)
- Ensure transparency of processes (*between Business, support organizations, and regulators*)

- Create a framework and a process that will allow the APD to better manage information and data assets
- Promote data quality through controlled continuous quality data improvement. (Reduce redundancy)
- Ensure appropriate use of data

These guidelines are in accordance with the following HIPAA/HITECH rules, NIST 800-53a Rev4 standards, and Safeguard standards.

The purpose of the table to provide the Issuers and/or TPA with the federal controls relating to the transmission, privacy and security of data and aligns with HIPAA/HITECH. It provides validation to our strict data management controls and safeguards.

Guidelines for Data Security				
Title	**Required or Addressable**	**Control Question**	**HIPAA Question**	**Tactical Remediation**
Acceptable use of assets	R	Have rules for the acceptable use of information and assets associated with applications been identified, documented and implemented?	**164.308(a)(7)(ii)(E)** Applications and Data Criticality Analysis (A): Assess the relative criticality of specific applications and data in support of other contingency plan components.	1015 Data Classification
Classification guidelines	A	Is information classified in terms of its value, legal requirements, sensitivity and criticality to the organization?	**164.308(a)(7)(ii)(E)** Applications and Data Criticality Analysis (A): Assess the relative criticality of specific applications and data in support of other contingency plan components.	1015 Data Classification
Information back-up	R	Are back-up copies of applications and their supporting information taken and tested regularly in accordance with an agreed back-up policy?	**164.308(a)(7)(ii)(A)** Data Backup Plan (R): Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.	1040 Business Continuity Planning (BCP) and Disaster Recovery (DR)
Information handling procedures	A	Have procedures for the handling and storage of information been established and do they protect this information from unauthorized disclosure or misuse?	**164.308(a)(7)(ii)(E)** Applications and Data Criticality Analysis (A): Assess the relative criticality of specific applications and data in support of other contingency plan components.	1015 Data Classification 1025 Secure Data at Rest and in Transit 1035 Data Release Management

Guidelines for Data Security				
Title	**Required or Addressable**	**Control Question**	**HIPAA Question**	**Tactical Remediation**
Exchange agreements	R	Have agreements been established for the exchange of information and software between the organization and external parties?	**164.308(b)(1)** Business Associate Contracts and Other Arrangements: A covered entity, in accordance with § 164.306, may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with Sec. 164.314(a), that the business associate will appropriately safeguard the information.	Educate on 10.0 Third Party Security Policy and 6.0 Security Monitoring and Response Policy
Electronic commerce	A	Is electronic information passing over public networks protected from fraudulent activity, contract dispute, and unauthorized disclosure and modification?	164.312(e)(2)i Integrity 164.312(e)(2)ii Encryption	1025 Secure Data at Rest and in Transit 1035 Data Release Program
Policy on use of network services	A	Are users only provided with access to the services that they have been specifically authorized to use?	**164.308(a)(4)(ii)(B)** Access Authorization (A): Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.	
User identification and authentication	R	Do all users have a unique identifier (user ID) for their personal and sole use, and has a suitable authentication technique been chosen to substantiate the claimed identity of a user?	**164.312(a)(2)(i)** Unique User Identification (R): Assign a unique name and/or number for identifying and tracking user identity.	

Guidelines for Data Security				
Title	**Required or Addressable**	**Control Question**	**HIPAA Question**	**Tactical Remediation**
Information access restriction	R	Is access to information and application system functions by users and support personnel restricted in accordance with the defined access control policy?	**164.312(a)(1)** Access Control: Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4). **164.308(a)(4)(ii)(B)** Access Authorization (A): Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. **164.308(a)(4)(ii)(C)** Access Establishment and Modification (A): Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.	1055 Secure Data in Non-Production Environments (de-identification service)
Output data validation		Is data output from an application validated to ensure that the processing of stored information is correct and appropriate to the circumstances?		1005 Information Security Governance 1050 Security Code Testing
Information leakage	A	Are opportunities for information leakage prevented and monitored?	**164.308(a)(5)(ii)(B)** Protection from Malicious Software (A): Procedures for guarding against, detecting, and reporting malicious software.	1015 Data Classification 1070 Incident Response Capability 1075 Data Loss Prevention (DLP)
Including information security in the business continuity management process	R	Has a managed process been developed and is it maintained for business continuity throughout the organization that addresses the information security requirements needed for the organization's business continuity?	**164.308(a)(7)(ii)(C)** Emergency Mode Operation Plan (R): Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.	1040 Business Continuity Planning (BCP) and Disaster Recovery (DR)

All Issuers and their Third Party Administrators are considered to be "Data Providers". The EIS is considered to be the "Data Consumer" in the context of this guide.

"Data sharing" is considered sensitive information or files provided by and to the EIS.

The expectation is that data provided to the EIS environment will be provided by the data providers after undergoing appropriate reviews and validations by the data provider. Prior to submission of any data or data files to the EIS, your evaluation will include at least two major components: an evaluation that the data provided can satisfy the purposes of the data elements required for the EIS and that the data sharing satisfies all applicable privacy and security regulatory constraints associated with the data.

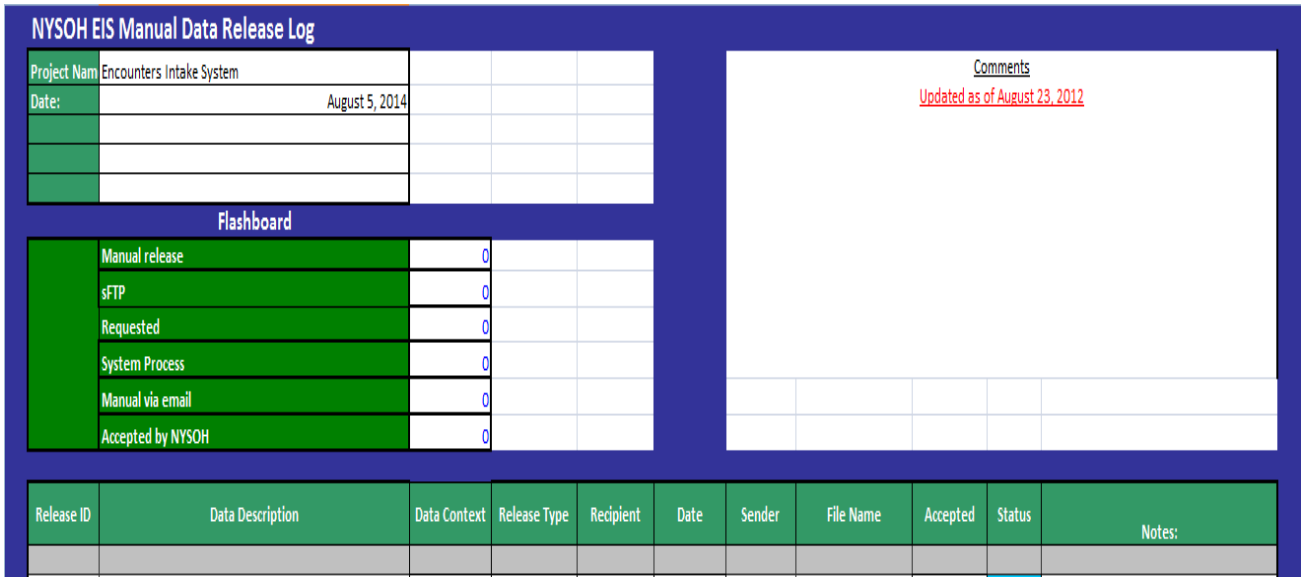
From a data security perspective, therefore, Issuers and their Third Party Administrators must understand the potential risk for creating confidential data sets from their production systems and must ensure that these data elements are exposed only in appropriate manners governed by agreements with the EIS, including but not limited to the EIS registration form and the Trading Partner Agreement.

The following is recommended for all data providers associated to the EIS.

1. Data Providers will apply all existing data security measures to the data submitted whether test or production appropriately. The submissions will provide federally-compliant levels of data encryption for data in motion and will provide sufficient information to identify the data transaction[1]. Data providers that are submitting potentially sensitive data sets authorize data release based on these standards and validations. The EIS will only be responsible for data once received from you and processed in any environment as long as the appropriate validations and confirmations are provided by the Data Provider.
2. The EIS will provide to the Data Provider specific formats and data structures and each provider must submit their files in these formats or all files will be immediately rejected and deleted from all environments and the data provider will be notified along with the Primary Issuer and the EIS contact.
3. Data providers are responsible for transforming the data into one of the standard data formats provided.
4. Operational business data stewards within your organization should work through various validation and quality issues prior to submitting files to the EIS.
5. Maintain a Data Release Management Registry (DRMR) of inbound and outbound data for validation and audit purposes. The DRMR should at minimum contain the following:
    a. *Data Description - This provides a means to uniformly describe data and validations performed.*
    b. *Data Context – This provides a means to ensure the EIS understands the type of data and its origin.*
    c. *Data Sharing - This supports the access and exchange of data for ad-hoc requests and fixed, re-occurring transactions between you and the EIS and ensures the appropriate people are receiving the data including the location sent to, individual contact at the EIS and date and time submitted.*

[1] A transaction for the purposes of this guide shall mean individual files provided for a single transmission. For example, one data transmission that contains 3 files is considered to be 3 transactions.

The table below shows the suggested manual data release log



NYSOH EIS Manual Data Release Log

Project Nam	Encounters Intake System
Date:	August 5, 2014

Comments

Updated as of August 23, 2012

Flashboard

Manual release	0
sFTP	0
Requested	0
System Process	0
Manual via email	0
Accepted by NYSOH	0

Release ID	Data Description	Data Context	Release Type	Recipient	Date	Sender	File Name	Accepted	Status	Notes:

Figure 4: Data Release Management Log

6. Each Data Provider should maintain a Registry (figure 1) of files going out to the EIS. This ensures a review is being completed on a regular basis and provides an audit log for sensitive information leaving the organization and in this case being submitted to the EIS.
7. Under no circumstance can you submit any data files associated to EIS via standard email services, you must submit via the designated SFTP services provided to you as part of your registration.
8. All data files; whether test or production submitted to the designated SFTP folder must follow the standard naming convention defined in Section 3.1.5 of this companion guide. Any files that do not meet this criteria will be immediately rejected and the Issuer or their Third Party Administrator notified promptly by the Primary EIS contact.
9. Once files meet the standards and are placed on the SFTP folder as defined in section 4.1, the EIS will perform a validation of the data content via an automated process and will look for certain indicators in the data content. If the file is correct, the EIS will process the file and accept the submission.
10. If the file is determined to be invalid or contains incorrect data; (for example a test file contains production data), the file will be deleted and the Issuer notified through the standard notification process. In order to minimize risk, the EIS is imposing that after two consecutive issues relating to data submissions where there is inherent risk, a recommendation will be made to disable the Issuer or Third Party Administrator account until such time as our team can determine the cause of the violation and discuss with the data provider. This is a mitigation measure to reduce any risks to the EIS platform and the data provider.

Proposed and recommended workflow:

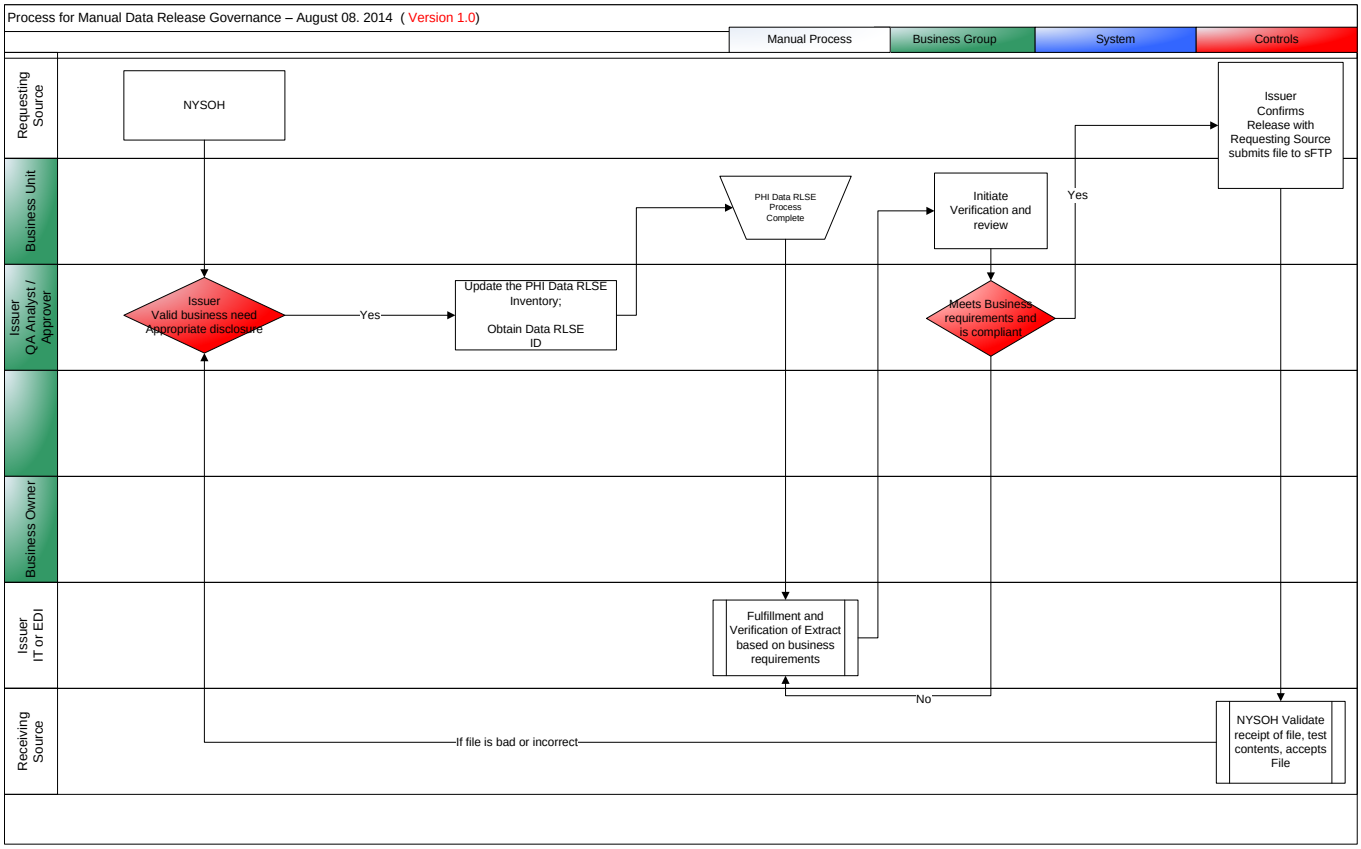


Figure 5: Process for Manual Data Release

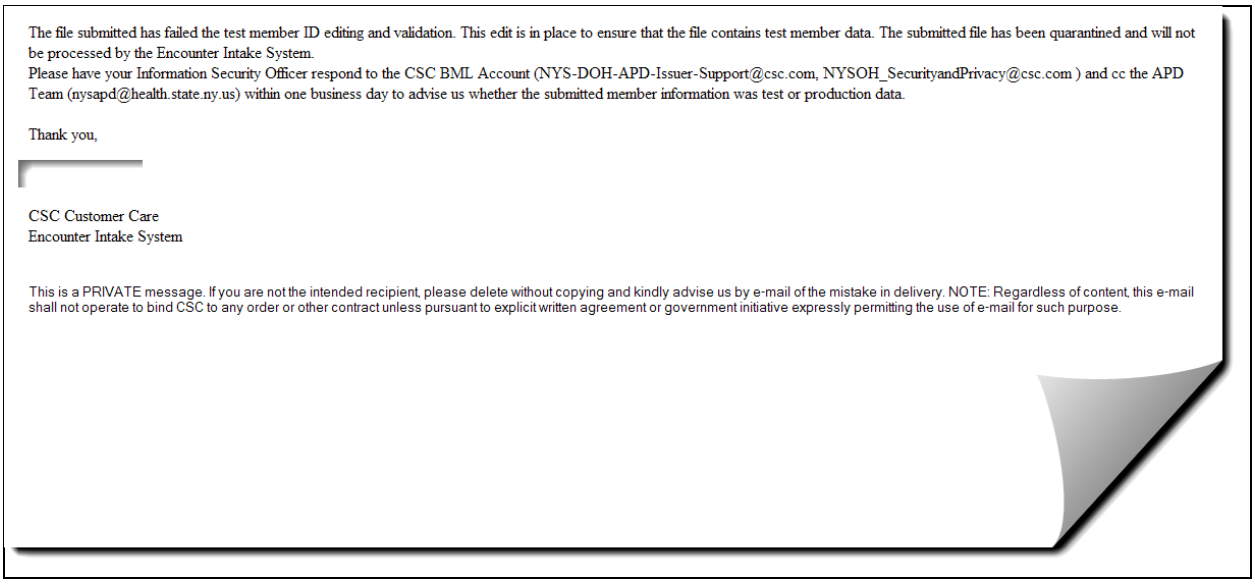
3.1.11 Contacting the EIS Information Security Officer

In the event you have questions or concerns relating to EIS information Security standards and safeguards please send an email to NYSOH_SecurityandPrivacy@csra.com to the attention of the Information Security Officer.

4 Test File Submission

All test files submitted to the EIS must use only the Member Test Data provided to the Issuer by the APD Team. In the event our systematic review process detects invalid member test data, the file will be quarantined and invoke our notification process to the EIS Information Security Officer, as well as the Issuer that submitted the data file.

The Issuer's Point of Contact (PoC) will be notified immediately upon a suspected or confirmed invalid file. The PoC will receive the following email.



The file submitted has failed the test member ID editing and validation. This edit is in place to ensure that the file contains test member data. The submitted file has been quarantined and will not be processed by the Encounter Intake System.
Please have your Information Security Officer respond to the CSC BML Account (NYS-DOH-APD-Issuer-Support@csc.com, NYSOH_SecurityandPrivacy@csc.com) and cc the APD Team (nysapd@health.state.ny.us) within one business day to advise us whether the submitted member information was test or production data.

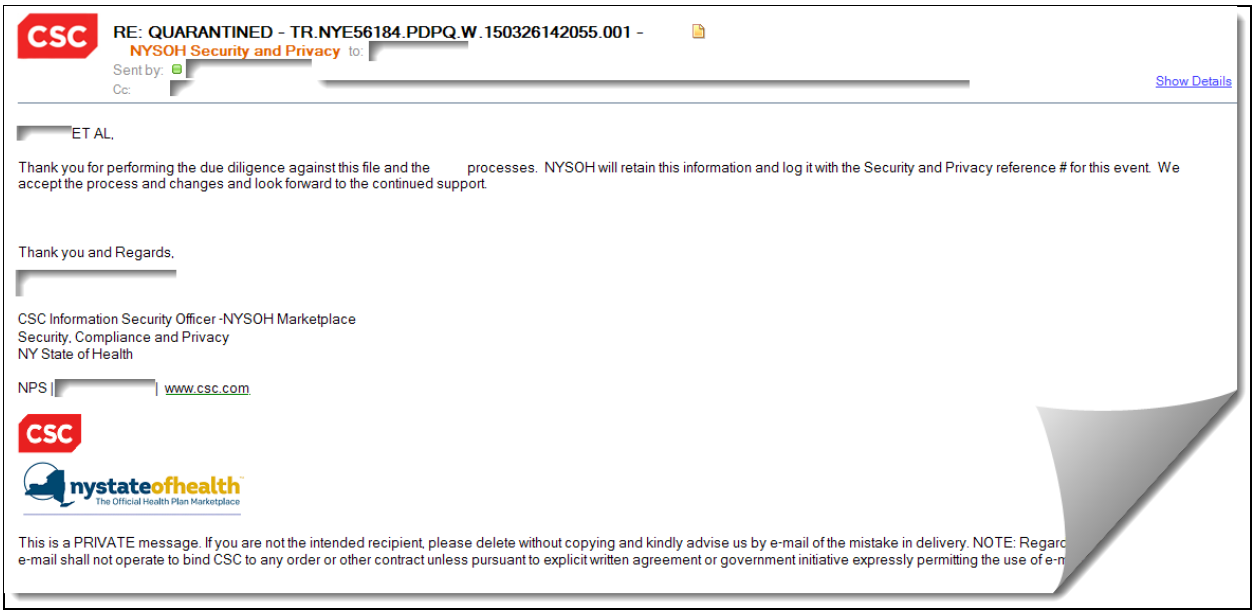
Thank you,

CSC Customer Care
Encounter Intake System

This is a PRIVATE message. If you are not the intended recipient, please delete without copying and kindly advise us by e-mail of the mistake in delivery. NOTE: Regardless of content, this e-mail shall not operate to bind CSC to any order or other contract unless pursuant to explicit written agreement or government initiative expressly permitting the use of e-mail for such purpose.

The Issuer will have one (1) business day to submit a root cause response and remediation plan to ensure or reduce the risk of inadvertent PHI disclosure into our test environment.

Each infraction is logged and assigned a reference number for auditing purposes and will be provided to the Issuer as part of the email response from the EIS Security and Compliance group via email.


RE: QUARANTINED - TR.NYE56184.PDPQ.W.150326142055.001 -
NYSOH Security and Privacy to:
Sent by:
Cc:
Show Details

ET AL,

Thank you for performing the due diligence against this file and the processes. NYSOH will retain this information and log it with the Security and Privacy reference # for this event. We accept the process and changes and look forward to the continued support.

Thank you and Regards,

CSC Information Security Officer -NYSOH Marketplace
Security, Compliance and Privacy
NY State of Health

NPS | | www.csc.com

nystateofhealth
The Official Health Plan Marketplace

This is a PRIVATE message. If you are not the intended recipient, please delete without copying and kindly advise us by e-mail of the mistake in delivery. NOTE: Regarc
e-mail shall not operate to bind CSC to any order or other contract unless pursuant to explicit written agreement or government initiative expressly permitting the use of e-n

In the event the Issuer has multiple infractions, the EIS Information Security Officer and the NYSDOH Legal Affairs office may request a meeting with the Issuer's Chief Information Security Officer to discuss the issue and determine the appropriate course of action to ensure the protection and privacy of the EIS information system and the consumer data.

5 Production Submissions

Trading partner profiles established during the enrollment process (defined in section 2.2.1 of this document) are the same for both the EIS production environment and the Pre-Production environment. Once an Issuer has successfully completed testing each transaction type, they will be approved to submit production files to the EIS. An Issuer will receive a confirmation email from the NYS APD team once testing has been successfully completed. The confirmation email will indicate when the issuer can begin submitting to production. Files submitted to the production environment (ending in .15) prior to approval being granted will not be processed. Successful testing is defined as being able to exchange encounter files with the EIS, submit at least 6 files with 40 or more claims having a claim acceptance rate of 90%, and to be able to process the associated response files.

5.1 Guidelines for Sending Production Files

Before submitting production files to the EIS, the Trading Partner must:

For X12 transactions:

- Verify the Trading Partner ID in data elements ISA06 (Interchange Sender ID) and GS02 (Application Sender's Code) is the Issuers HIOS ID or TPA ID.
- Verify the value in ISA08 and GS03 is 'NYSOH-ENC'.
- Verify there is only one ISA/IEA per file.

- Verify that there is only one Functional group (GS/GE) for each envelope (ISA/IEA).

For NCPDP transactions:

- Verify the Trading Partner ID in the Sending Entity Identifier fields in the History Header Record.
- Verify there is just one Header Record (PA) and one Trailer Record (PT).
- Verify there is at least one Detail Record (DE).

For all transactions:

- Limit the file size to 50 MB per file.
- Apply a unique file name with no spaces or special characters in accordance with the file naming conventions listed in Section 3.1.5.
- Upload the production file to the inbox associated with Production IP address (ending in .15) assigned by the EIS during initial enrollment.
- Set the appropriate production indicator on the inbound file (P). Example:

  ASC X12 Transactions For all ASC X12 Transactions set the Usage Indicator (Data Element ISA15) to a value of "P". Example:

  ISA*00* *00* *ZZ*Test Prof1 *ZZ*NYSOH-ENC *010806*1200*^*00501*000000008*1***P***:~

  NCPDP Transactions (Batch Only)

  Setting the Batch Header File Type (702-MC) to a value of "P"

5.2 Production Availability

The production environment is available 24 hours a day, 7 days a week.

5.3 File Naming Convention

For proper file naming convention, see Sections 3.1.5 and 3.1.6.

5.4 File Processing

Files processed in production follow the same path outlined in Section 3.1.7.

6 Resources

Useful Websites

The registry for the NPI (National Provider Identifier) is the National Plan and Provider Enumeration System (NPPES), at:

https://nppes.cms.hhs.gov/NPPES/Welcome.do

Other resources pertaining to the National Provider Identifier:

http://www.cms.hhs.gov/NationalProvIdentStand/

Implementation Guides and Non-medical code sets are at:

http://store.x12.org/

The HIPAA statute, Final Rules, and related NPRMS (Notices of Proposed Rulemaking) are available at:

http://www.cms.hhs.gov/HIPAAGenInfo/

http://aspe.hhs.gov/datacncl/adminsim.shtml

Information from CMS about ICD-9 and ICD-10 codes:

http://www.cms.hhs.gov/ICD9ProviderDiagnosticCodes/01_overview.asp#TopOfPage

https://www.cms.gov/ICD10/

Quarterly updates to the HCPCS code set are available from CMS at:

http://www.cms.hhs.gov/HCPCSReleaseCodeSets/

(CPT-4, or Level 1 HCPCS, is maintained and licensed by the American Medical Association and is available for purchase in various hardcopy and softcopy formats from of variety of vendors.)

Information at the Federal level about Medicaid can be found at:

http://www.cms.hhs.gov/home/medicaid.asp

The CMS online Manuals system includes Transmittals and Program Memoranda at:

http://www.cms.hhs.gov/Manuals/

Place of Service Codes is listed in the Medicare Claims Processing Manual and is maintained by (CMS), available online at:

http://www.cms.gov/Regulations-and-Guidance/Guidance/Manuals/downloads/clm104c26.pdf

Information Security and Standards:

NIST 800-53a Rev4 Publication:

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf

National Institute of Standards and Technology:

http://www.nist.gov/

Accounting for Disclosure:

http://www.gpo.gov/fdsys/pkg/FR-2011-05-31/pdf/2011-13297.pdf

7 Trading Partner Information Change Summary

Version	Date	Section(s) Changed	Change Summary
1			Draft version of Trading Partner Information Companion Guide for Encounters
	8/28/2014		Address feedback from DOH
1.0	9/3/2014	3.1.8 3.1.9 3.1.10	X12 Submission / Acknowledgement / Response Process Updated NCPDP Submission / Acknowledgement / Response Process Updated Reformatted Guidelines for Data Security Table
1.1	1/6/15	1.3 2.3 3 4	Revised Overview to include NCPDP transactions Updated Guidelines for using SFTP Updated Testing Information Updated Production Submission Certification criteria
1.2	4/2/15	2.2 2.3 3 3.1.5 3.1.6 3.1.8 4	Revisions for Release 2 – Medicaid/CHP Managed Care Plan Reporting Revisions for quarantined test file submissions
1.3	8/3/2015	1.5 2.2.1 2.3 3. 3.1.5	Clarify process for Issuer Portal access requests Correct grammatical/typographical errors. Removed specific reference IP address endings Correct grammatical/typographical errors. Removed unnecessary sub-heading
1.4	10/5/2015		Correct grammatical/typographical errors.

Version	Date	Section(s) Changed	Change Summary
1.5	1/24/2017	 5.	Correct grammatical/typographical errors. Update State & CSRA contact information. Revisions for Release 3: Essential Plan Reporting Clarify approval process for Production submissions.
1.6	7/11/2017	Cover Page	Added NYS DOH APD Logo. Revised title language.