The HIPAA Eligibility Responder

Table of Contents

1 Introduction

1.1 The Eligibility transaction

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 prescribed the 270 and 271 X12 EDI transactions for the transmittal of eligibility data. Checking the eligibility of insurance coverage is an essential operation in health care. Doctors should know by the time they see a patient whether the patient is covered, if there are co-payments to be collected and whether coverage for a certain diagnosis is included.

The 270 EDI transaction is the request for eligibility information. Typically a provider would take the patient information and then compose the request message. He would then expect a 271 EDI response message. EDI transactions that begin with a '2' are real-time transactions. That means that the response is expected within 20 seconds.

HIPAA implemented this differently at first and did not mandate real-time responses for any transaction. Having the response by 7 am the following day was acceptable. The Accountable Care Act (aka Obamacare) tightens this requirement.

Nevertheless, in planning your HIPAA solution you should strive for real-time execution of the 270/271 as well as the 276/277 claim status information.

What is a response?

The basic functionality between 270 and 271, between the request and the response is important to understand. Though request and response should be linked, this is often not possible and a generic answer is returned.

Here are some different scenarios:

Manual Mode:

1: Provider has a generic request asking for service type code 30. (health plan coverage) This seems to be the encouraged version by the implementation guide. We can give a

a) Quick response with service type code 30 and optional dates

b) Rejection for different reasons

c) Detailed response listing all available benefits

2: Provider is specific and has a detailed request. Maybe he/she specifies procedure codes and diagnosis and has inquires about several benefits employing multiple loops 2110D or 2110C. This is the idealized case on the request. If the request is the same for

several service type codes, they can be repeated within EQ_01. For the response we can have several scenarios:

a) Quick response. Yes, you can even on the most detailed request just give a quick response and get away with it

b) Rejection

c) No matter how complex the request, you create your standard response, listing all available benefits

d) Each loop 2110C/D in the request is answered in detail with a loop 2110C/D in the response. The EB_03 segment of the response mirrors the EQ_01 segment of the request.

i) Single service type code in EQ_01 <-> Single service type code in EB_03, one request loop answered by one response loop

ii) Single loop with Multiple service type codes in EQ_01 <-> answered by multiple service type codes in EB_03, one request loop answered by one response loop

iii) Single loop with Multiple service type codes in EQ_01 <-> answered by multiple loops 2110C/D, each service type described as needed

The HIPAA Eligibility responder is able to serve all these scenarios, but, we should be clear that case 2.d.ii and 2.d.iii can get infinitely complicated and complex and should be avoided.

The quick response is the easy way out. We support it for sure.

The most common case in the industry is 1.c and 2.c; **No matter what the request, simple or complex, the response lists all the available benefits and their limitations as specific as possible.**

Case 2.d.i is possible for a trained and dedicated case worker to provide a very specify response with the HIPAA Eligibility Responder but it will take time to get efficient and gain a deep understanding of the process.

We spent a lot of thought on the matching of EQ_01 to EB_03 (Service Type Codes)

requirements. We won't limit the software to this case alone. EB_03 **does not** have to match EQ_01 and you should be able to change the Service Type Code. The EQ_01 value is pre-loaded on the response form into combo box. We can have requests with multiple EQ loops but we won't have to answer them all.

Auto-Processing:

No matter what the request, simple or complex, the response lists all the available benefits and their limitations as specific as possible.

This motto will be the case in the Auto-Process especially. The computer cannot make diagnosis and procedure specific decisions.

One of my objectives for the development of the HIPAA Eligibility Responder is to provide an automated process with an easy configurable interface, so that these real-time transactions can be automatically returned within seconds.

You might have seen the database menus. That's part of this development and the following is for your information.

The HIPAA Eligibility Responder will query a database table "ACTIVE.MEMBERS" where the covered members and dependents are listed. Just 10 fields or so to uniquely identify the member and match the request with certainty. This members table is linked to the defined benefits. It will be updated daily by the Administrator.

- HIPAA Eligibility Responder reads the request
- finds the subscriber and/or patient if different and gets a link to the benefits.
- Then it returns all defined benefits or returns a rejection :AAA rejection code when the member is not found for example.

There are three ways to link to benefits:

1. Our users have to pre-define benefits and the ActiveMembers table has a field that contains a list of those benefits
2. The member ID is the foreign key to the DefinedBenefits table and each member's benefits are populated together with their defined benefits in an upload

3. The ActiveMembers file has one 255 byte field which contains an EDI string with the benefits. Customer has to write his own logic to formulate benefits in the 271 format. All business logic is under the customers control within a stored procedure that returns either AAA or the benefit segments.

1.2 The HIPAA Eligibility Responder

Before a provider renders medical services to a patient, he/she wants to know if this service is covered by an insurance policy. Traditionally this has been handled by telephone operators or voice response systems with fax back options. HIPAA was conceived to bring administrative simplification into the provider-payer relationship and was intended to lower the cost of doing business for payers and facilitate the communications between payer and provider.

EDI, Electronic Data Interchange, revolutionized many industries. Banking exploded in the last 30 years due in large part to the effectiveness of electronic transactions. Every time you charge, every time you get cash from an ATM machine you invoke electronic transactions. The health care industry came very late to this new business tool and was forced into EDI by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) which mandated that every payer and many providers had to be able to communicate through EDI. With lots of kicking and screaming the law was finally implemented 1/1/2003 and now 10 years later more than 90 percent of medical claims are transferred as EDI. The other transactions limp, like payment advice and eligibility are somewhat behind but they too are increasingly becoming the tool for the business transaction they were designed for.

The 270 eligibility request transaction is designed to let a provider transmit patient information that clearly identifies a particular patient and inquires about the policy coverage of the services in question. Even multiple benefits can be requested and diagnosis codes can be included. A payer's EDI system would parse out the request, look up the membership records, find its eligibility status and transmit it back with the 271 eligibility response transaction listing existing coverage.

While this approach is straight forward, it is not easy to implement into an existing information management system and if the volume of 270 requests is low or even non-existent, then it would be sometimes unwise to spend a lot of money and resources on the automatic handling of eligibility requests.

This is where the HIPAA Eligibility Responder comes in. This software was designed to

parse out a 270 eligibility request file and allow the manual entry of eligibility response information. It would then use the request information to construct a 271 response transaction, ready to be sent back to the inquiring provider. The HIPAA Eligibility Responder is a low cost solution designed to bring a payer or any other covered entity into compliance with the HIPAA law.

The HIPAA Eligibility responder can work together with any SQL compliant database. Eligibility requests can be exported into the database and a process to look-up member benefit status is available. The implementer will have to populate the eligible benefits tables from their database.

1.3 Features

Here is a list of the features of the HIPAA Eligibility Responder:

- Takes in X12 270 EDI files, version 4010 and 5010
- Parses the whole file and lists each individual request
- Allows to answer requests sequentially or randomly from the listing
- Editable code sets, so you can set the codes used by your company and delete codes not applicable
- Allows to configure very specific and multiple benefits, utilizing the full breadth of the 271 transaction set
- Quick Response option to return the HIPAA minimum information that the 271 transaction allows.
- Request rejection on multiple level in accordance with the implementation guide
- After eligibility status assignment the program will create one 271 file that can be returned to the sender
- Exports information to any ODBC/SQL compatible database
- Retrieve eligibility information and create 271 eligibility response transaction
- Part of a CORE Phase I and II compliant solution in conjunction with the HIPAA RealTime Server

1.4 Requirements and Versions

When you download the software you are confronted with a choice of 32 bit and 64 bit versions.

The 32 and 64 bit respectively refers to the Windows operating system and the processor in your hardware. Since the early 1990's computers, hardware and software, were running in a 32 bit wide bus. That means 32 individual pieces of information could be processed as one. This was then a great jump from the previous 16 bit and in the early

days 8 bit processors. Translated to an example. the biggest 8bit number is 256. That's the highest number early computers could work with without engaging in some wizardry. 16bit brings us to 32,768. 32 bit to 2 billion which is good until now. In more recent years we have seen 64bit computers emerge. Their memory and number capability is near unlimited and all major operating systems are now available to run on this new 64bit hardware.

For programmers this opens new possibilities while also confronting us with the necessity to support two versions of the software. Fortunately this is solved by Microsoft with an integrated development environment that allows you to write one set of code and create two sets of installations. The HIPAA Eligibility responder is written in Visual Studio 2010 and needs the .Net framework 4.0. The installer checks for the presence of the framework and will download it from Microsoft and install it if necessary. Programs based on .Net architecture are resource hungry. We recommend a powerful workstation with Windows7 or Vista.

If your computer has a 64 bit operating system, you should use the 64 bit version of the HIPAAsuite software. It will better utilize the available resources. The 32bit version will also run though.

If you have a 32 bit computer, you can only run the 32 bit version.

2 Installation

2.1 Obtaining the Software

The HIPAA Eligibility Responder can be downloaded from the HIPAAsuite's website at www.HIPAAsuite.com. In addition, a CD with the software can be ordered directly with HIPAAsuite.

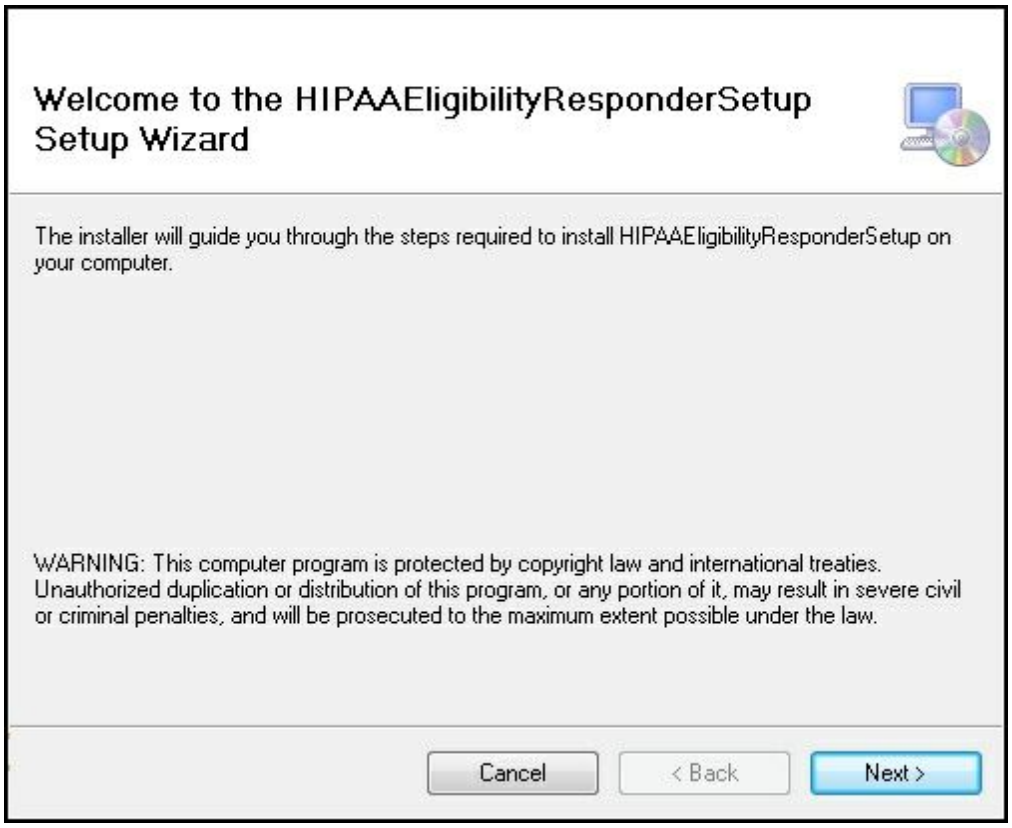
The software is in trial mode when first installed. After the end of this period it will stop working and can only be unlocked by either an extension of the trial for another 15 days or by purchase. A permanent key will put the HIPAA Eligibility Responder into full production mode.

2.2 Installing the Software

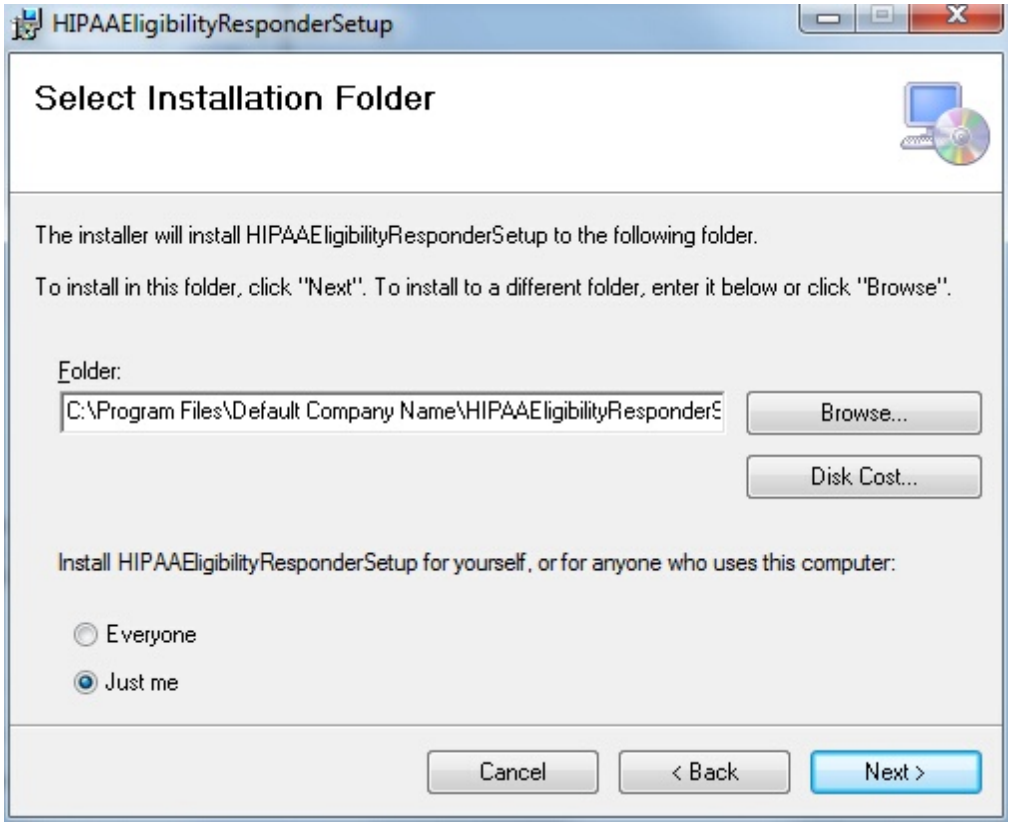
The software comes packaged as a zip archive 'HIPAAEligibilityResponderSetup.zip' Inside are two programs

- setup.exe, a program that checks if the necessary .Net frame work is installed on the computer. If not then the setup program will go to Microsoft's web site and update your computer. This might require a reboot
- HIPAAEligibilityResponderSetup.msi. This Microsoft Windows Install Script (msi) file contains all the necessary files that are contained in the package and the Microsoft Installation engine will sort out merge modules and dependencies of system files and other dll's.

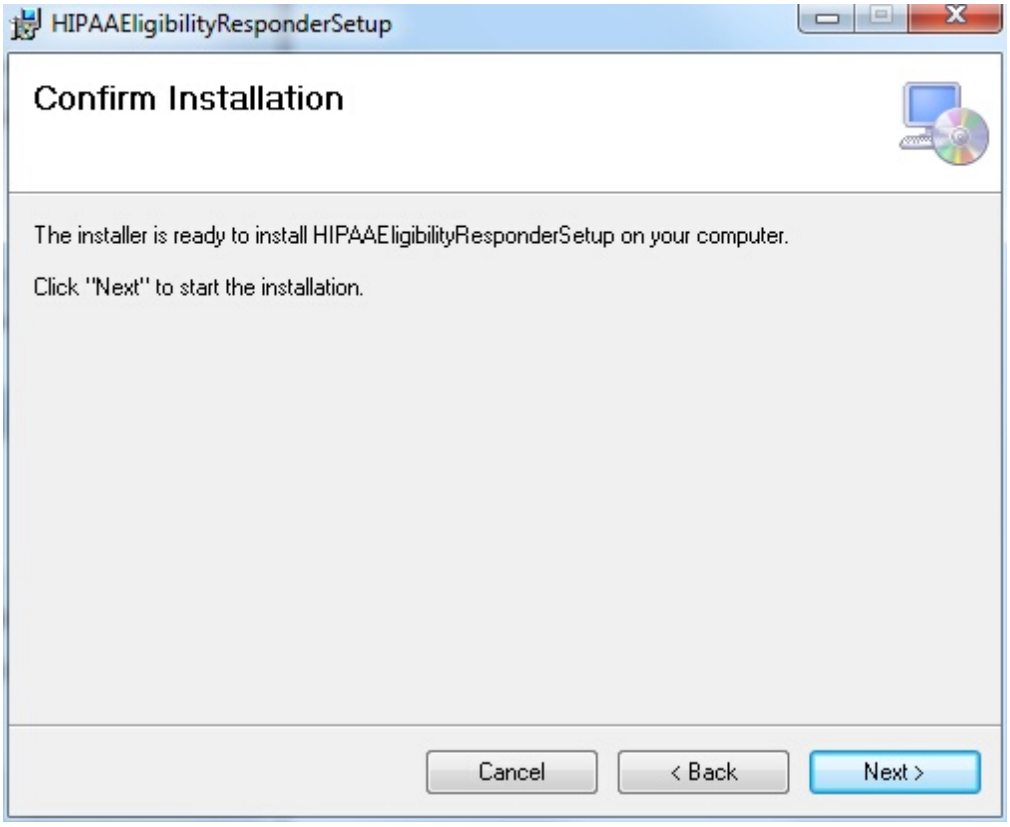
Below are the screens that you will encounter through the installation.



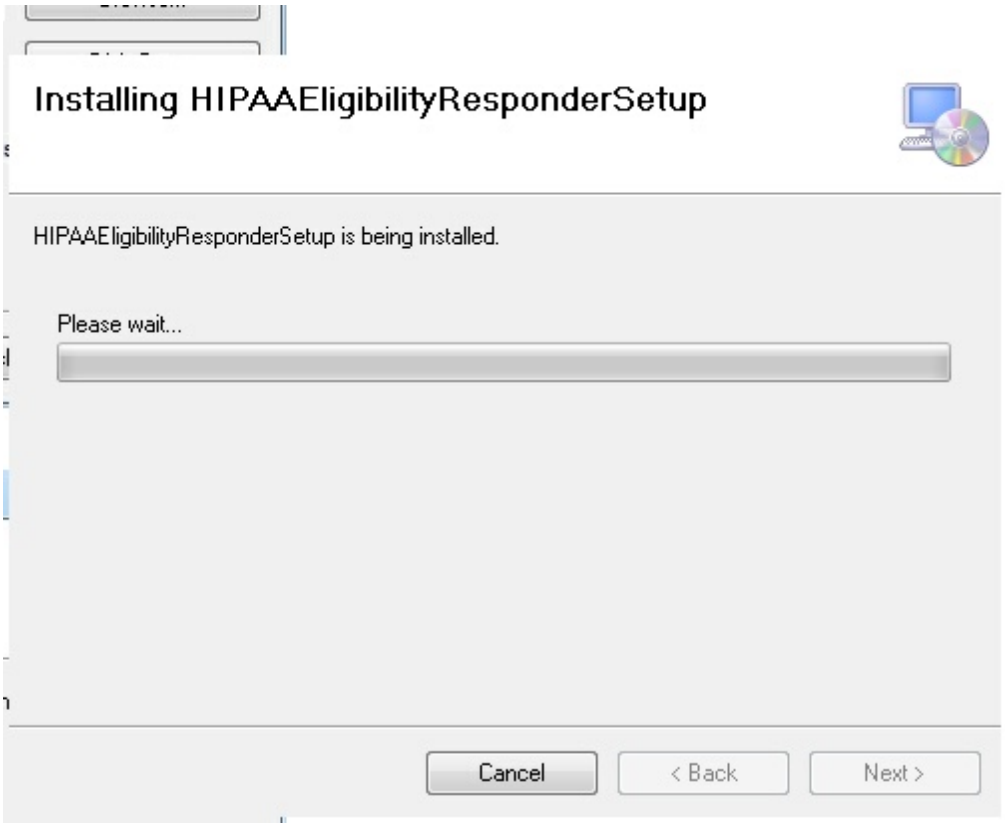
The first installation screen



The second screen



The third screen



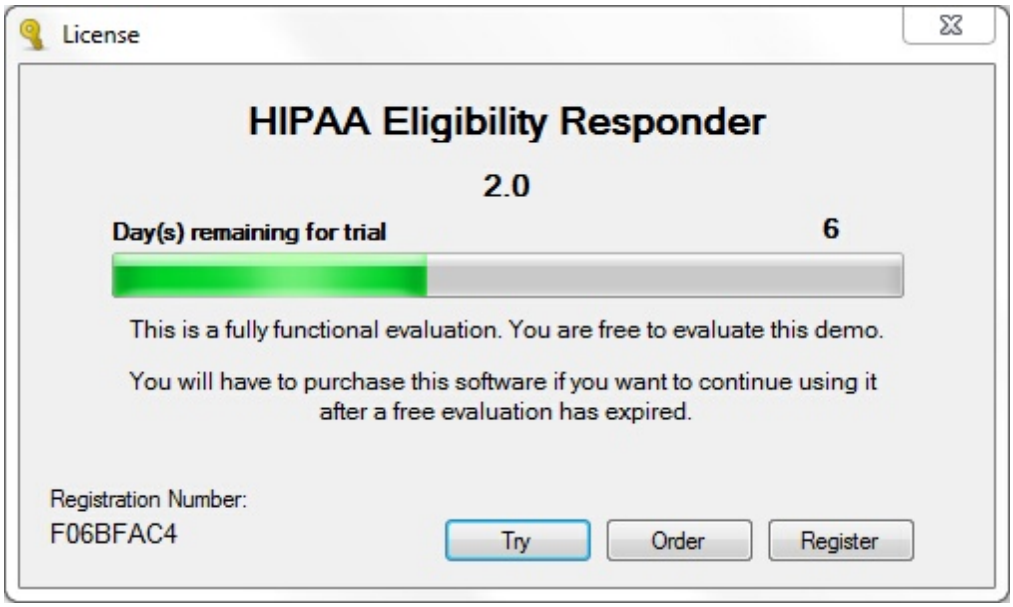
The fourth screen

2.3 Software Trial

The HIPAA Eligibility Responder comes with a free trial of 14 days.

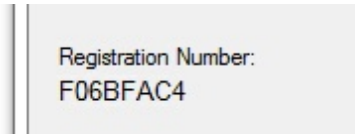
Should your trial time expire and you wish to continue your testing of the software, please send an email to info@HIPAAsuite.com with the Registration number and we will give you a trial extension.

If the product is not registered and you start it, you will see first the trial screen.



The software trial screen

You can see clearly the registration number in the lower left hand corner.



The Registration number

This number is needed for the registration as well as trial extension. It is unique to your computer and hardware. **You can copy the registration number to the clip board**, just hover with the mouse over it, so that you can easily paste it into an email. This avoids human error. (There are no 'O', the letter in the number, only zeros!)

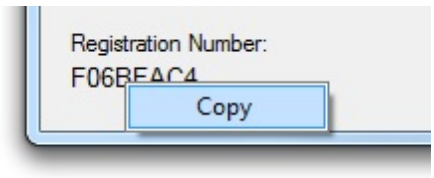
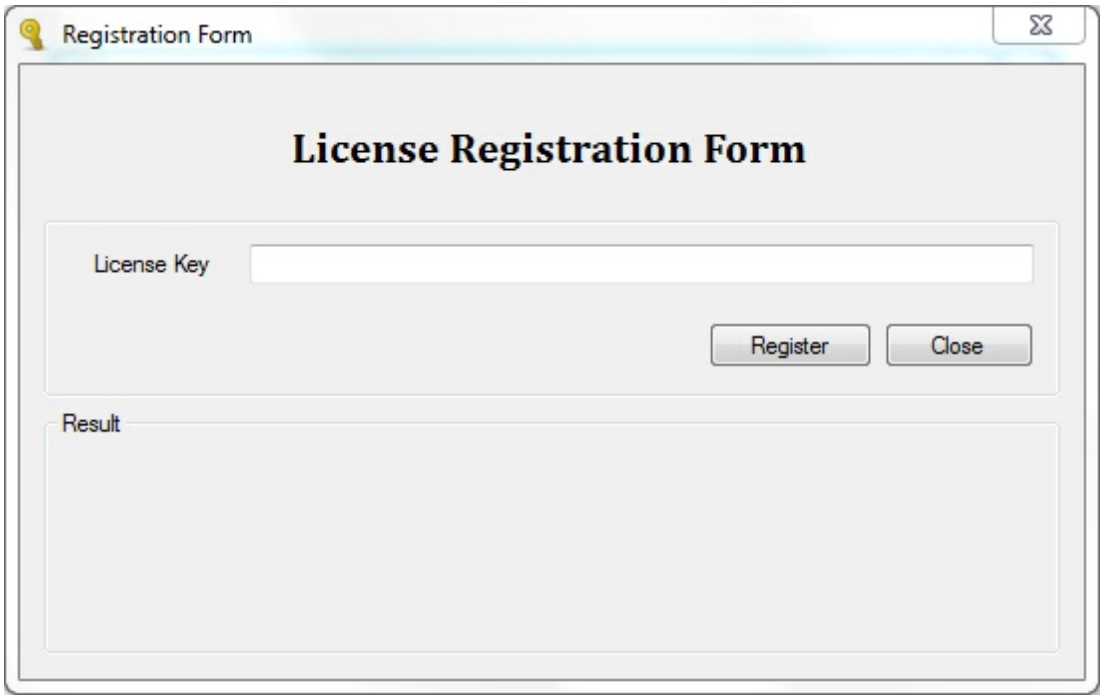


Figure3: Copy the registration number to the Windows clip board by hovering over it with the mouse

Trial extensions

We don't mind extending your trial if you need extra time to evaluate the software. You need to send us the registration number and we will gladly give you another 15 day trial.

Once you have an unlock key provided by us, you can register the product. Just click on the 'Register' button and you will see this screen



Registering the software

Enter the License Key as supplied in our email. This field is case sensitive. The best way is to copy and paste the information from our email.

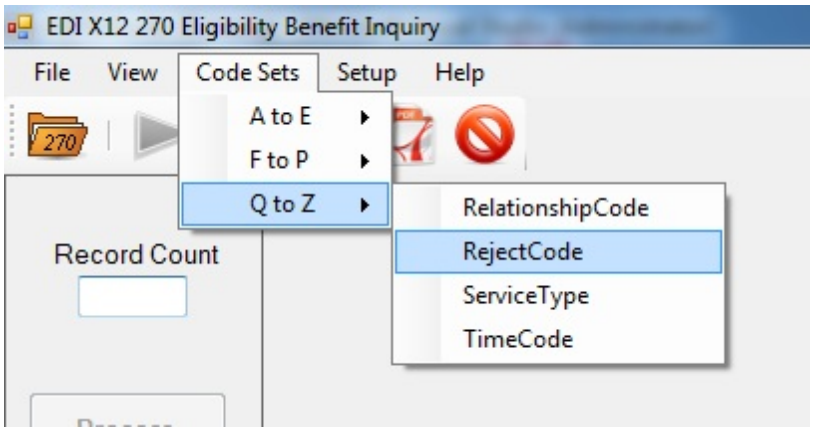
Once the product is registered with a permanent unlock code, future upgrades will find this key and install without further action necessary.

3 Setup

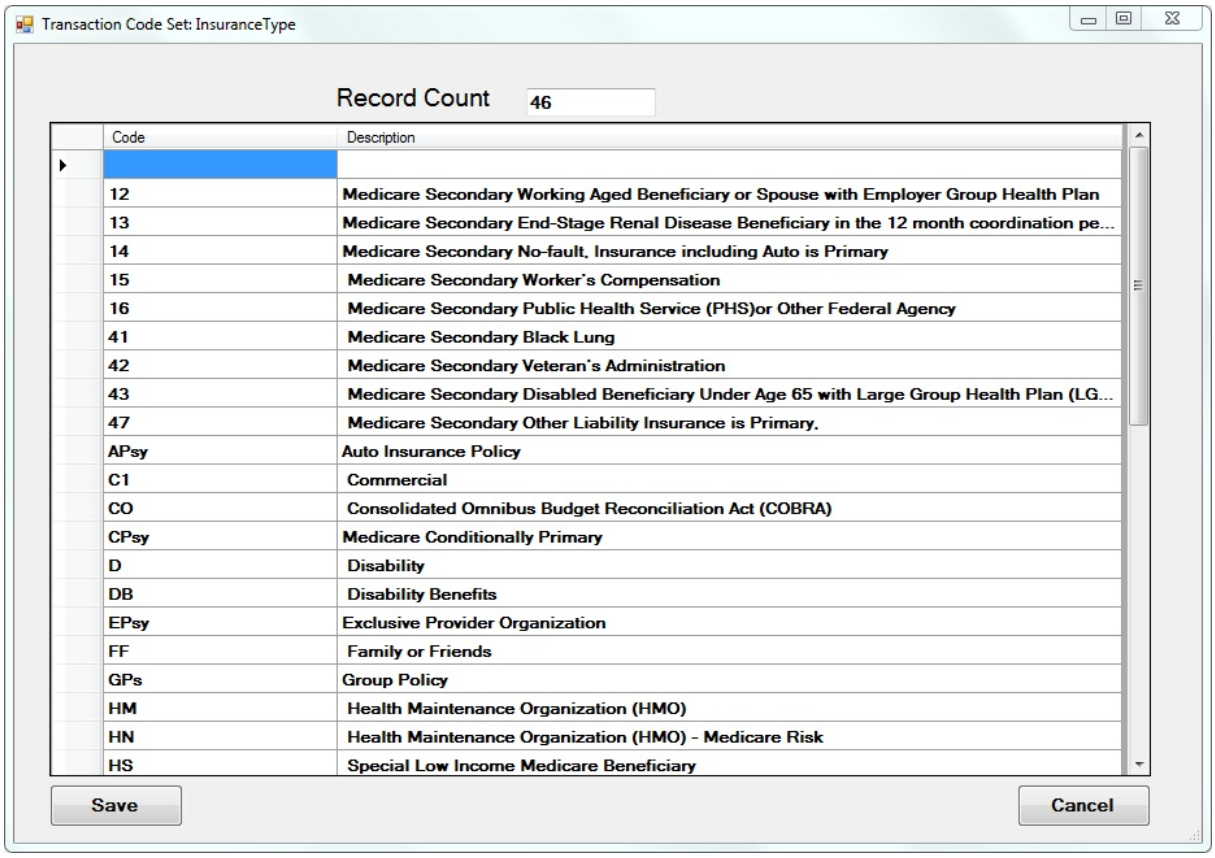
3.1 Code Sets

EDI relies on transaction code sets. These codes represent longer explanations and descriptions. At the onset of EDI one of the main design ideas was to make the EDI files as short as possible and to allow different languages to use the same descriptions by reducing long verbose explanations to 2-3 byte long codes. Computer storage was incredibly expensive and making any file larger than it absolutely had to be was considered wasteful.

The main menu of the HIPAA Eligibility Responder has the item 'Code Sets'. Click on it and sub menus will lead you to the individual code sets that the Eligibility Responder uses. The code sets are stored in the file codesets.xml in the 'Configuration' subdirectory of the Program Data section of the HIPAA Eligibility Responder, usually C:\Program Data \HIPAAsuite\HIPAAEligibilityResponder\Configuration\Codesets.xml



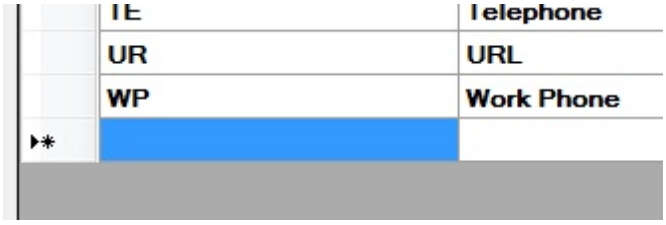
The Transaction code sets



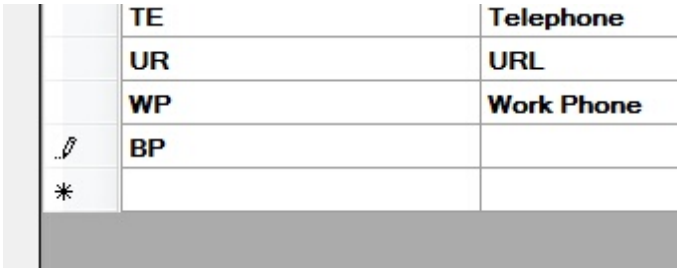
The code set editor

You can add, delete or edit codes.

To Add you type into the last row, and you see the grid change first into selected mode and when you click it again you are in edit mode. Now write your text. Note: Only after you leave this row will the changes take

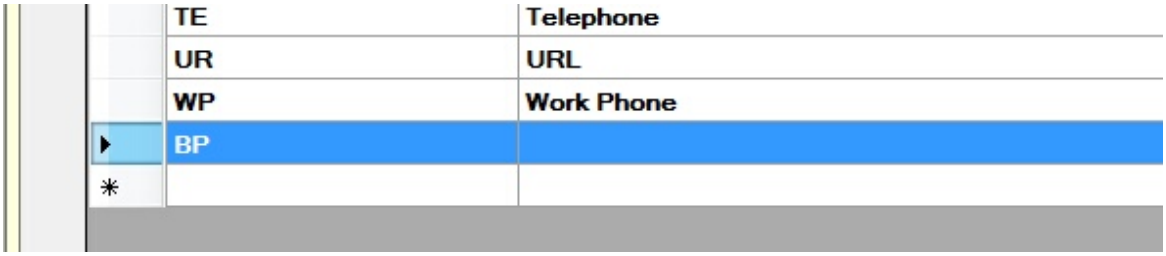


click into the last row and the cell is high-lighted



Click again and you are in edit mode. See the little pencil symbol

To delete, click into the margin and high-light a row. Now press the delete key on your key board



Highlighting a row by clicking into the left margin

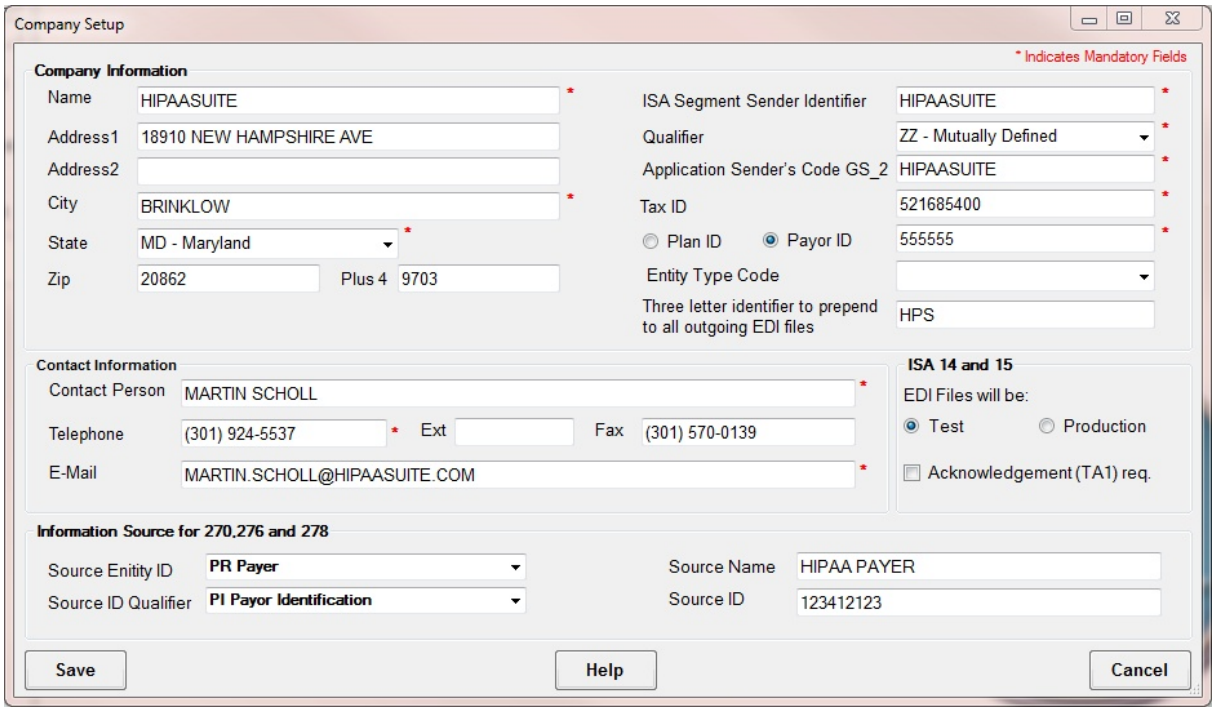
To edit, click into the cell that you want to change and make your changes. clicking or moving outside this cell makes the changes 'stick'

Don't forget to Save your changes by pressing the 'Save' button.

3.2 Company Setup

The HIPAA Eligibility Status Responder needs information about the Sender of EDI transactions so that the software can create a valid EDI file.

The menu item 'Setup --> Company Setup' will present you with the following screen:



The Company Setup window

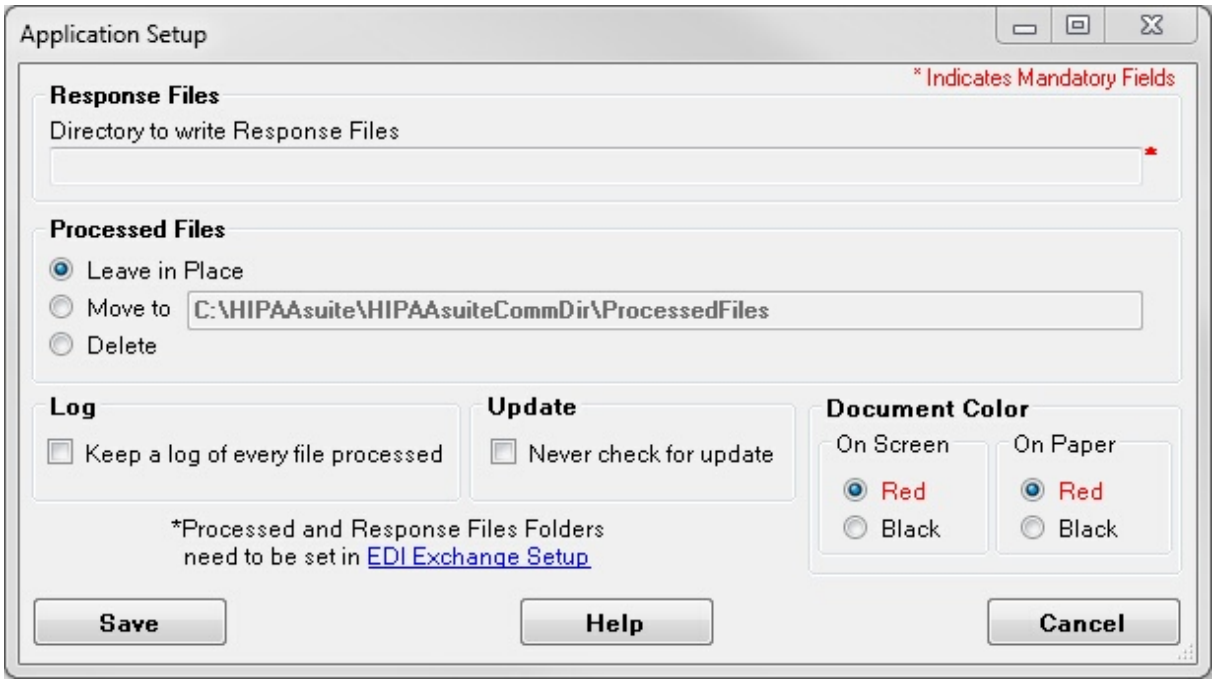
Fill in the information as far as you know it.

- Name and Address are self explanatory
- The ISA identifiers are needed create the outer EDI envelope, the ISA segment. If you don't already have an EDI identifier, choose it careful. It should be unique and easily identify your organization. You can use any name there with 15 character or less and use the qualifier 'ZZ' or choose another qualifier from a list below. Your company might already have a Duns ID or any other of those ID's.
  - o **01** **Duns (Dun & Bradstreet)**
  - o **14** **Duns Plus Suffix**
  - o **20** **Health Industry Number (HIN)**
  - o **27** **Carrier Identification Number as assigned by Health Care Financing Administration (HCFA)**
  - o **28** **Fiscal Intermediary Identification Number as assigned by Health Care Financing Administration (HCFA)**
  - o **29** **Medicare Provider and Supplier Identification Number as assigned by Health Care Financing Administration (HCFA)**
  - o **30** **U.S. Federal Tax Identification Number**
  - o **33** **National Association of Insurance Commissioners Company Code (NAIC)**
  - o **ZZ** **Mutually Defined**
- Application Sender's Code is the information that goes into the GS_02 element. You can repeat your ISA identifier here or if your company has different EDI processes, put HIPELIGRSP to identify the HIPAA eligibility responder as originator

- Tax ID is a required field and represents your companies tax payer ID
- In order to uniquely identify your files it is helpful to prepend a three letter code in front of the filename
- Entity Type code holds information that goes into the NM1_01 of the 2100 loop and classifies your business. There are 5 different choices to make
  - o Third Party Administrator
  - o Employer
  - o Gateway Provider
  - o Sponsor
  - o Payer
- Contact information again is self explanatory.
- ISA 14 specifies whether your files are Test of Production files
- Acknowledgement requested means that you expect a TA1 Acknowledgement in response to your file. Normally you would not.

3.3 Application Setup

When you select the menu item 'Setup --> Application Setup' you will see the following screen:



The Setup screen

Here you can select important settings for the application.

First there are paths to two important folders:

- The output directory. This is the folder where response files will be created in.
- The processed file directory. If you want to move your request files after they have been processed into an archive folder and get them out of the way, this is your folder

Then you can

- Determine whether you want to write every file processing to the log file, even manually processed files. We recommend this setting.
- HIPAAsuite products always check for the availability of product upgrades. If you find this annoying and the current version works for you, you can turn off the update check
- You can select the document color on screen and on paper for better readability

The last note refers to the EDI Exchange module. If it is licensed and activated then the two directories are set through EDI Exchange's setup

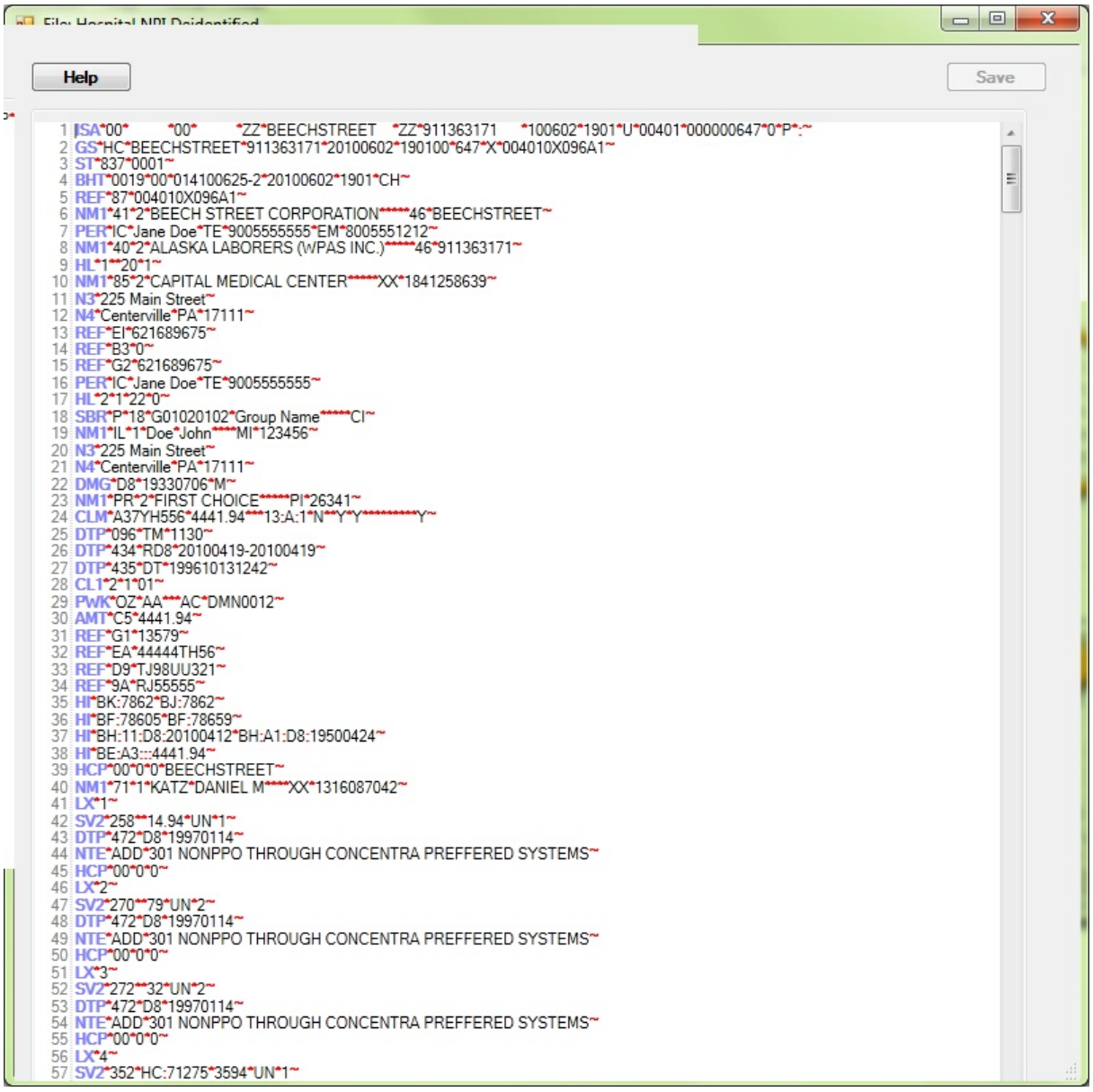
3.4 The EDI File Editor

Under the menu item 'View' you have the option 'EDI Editor' plus you have the EDI icon on the toolbar to invoke the EDI Editor.

EDI files are often hard to read, especially if they have no carriage returns and line feeds to put each segment on a line of its own.

This option is only enabled when you have Opened an EDI File

When you click this menu option, the following screen will appear



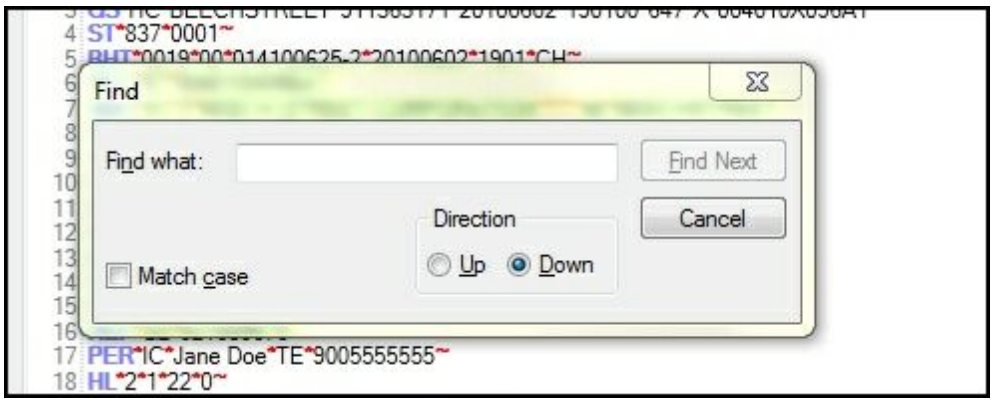
The EDI Editor

This Editor will replace all Element separators with a star '*', all sub element separators with a colon ':' and all segment separators with a tilde '~' even if the original file uses different delimiters. As long as you don't save, there will be no changes to the file.

When you right-click anywhere in the text, a floating menu will appear with typical test edit options such as cut, copy and paste,

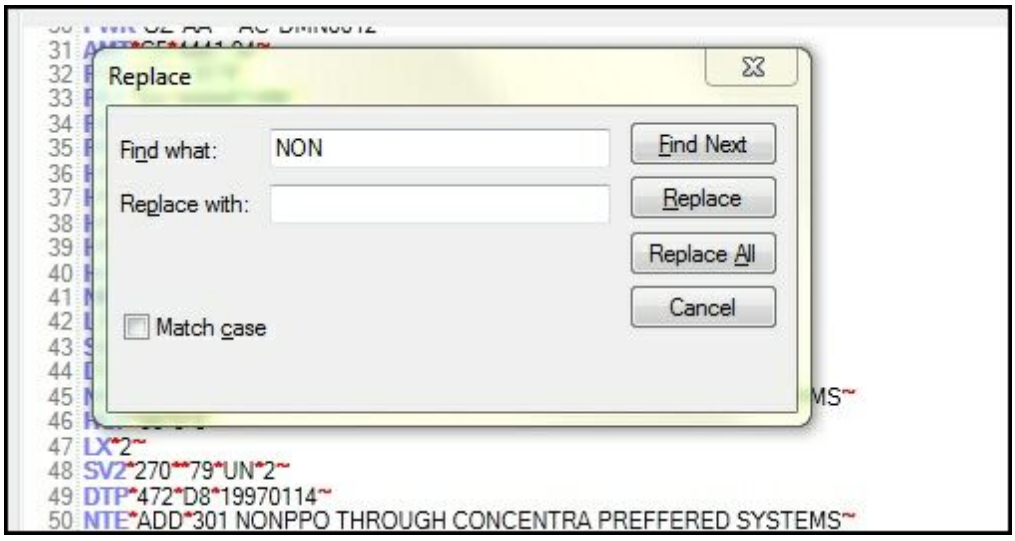
The floating menu of the EDI editor. right-click anywhere in the text to make it appear

Ctrl-F brings up the text search utility



The search utility

Ctrl-H will bring up the replace utility



The Find and Replace utility

If you make changes to the file, the 'Save' button becomes enabled and you can save any changes. The HIPAA Claim Master will further work with those changed files, you don't have to open the file again.

Changing EDI files can be a tricky undertaking. You should be experienced in the format of the 837 and understand that an 837 claim file could be a legal document that should not be altered without the consent of the originator.

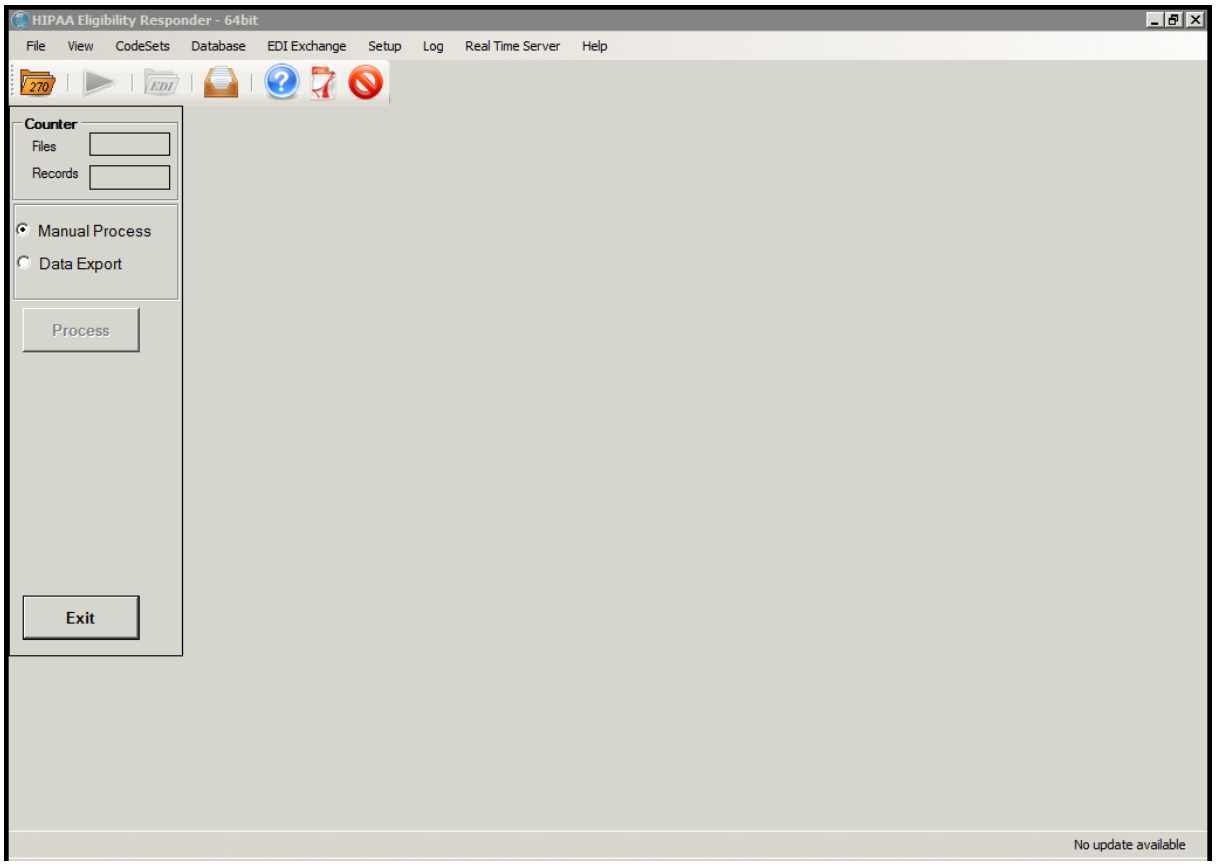
4 Using the Software

4.1 Running the Program

The installation will add a new group called 'HIPAAsuite' under your Start --> Programs listing. When you click on the HIPAAsuite listing a sub listing called Eligibility Responder will show. Click on it and the program will start.

The first thing you will see is the splash screen that indicated you are operating the HIPAA Eligibility Responder in trial mode. Note the Registration number in the lower left corner. This number is needed to create the unlock code for the unlimited use of the product. Hint: You can right-click the registration number and copy it to the clip board. This will avoid typos when you send the number to HIPAAsuite for the unlock code creation.

Once you click on 'Try' or when the software is licensed, immediately the main screen shows



The main screen of the HIPAA Eligibility Responder

When the program starts up it checks automatically at HIPAAsuite's web site if an update is available. If it finds an update you will be offered to download and install this update.

The menu bar on top gives you access to all the functionality of the software.

4.2 Opening an EDI File

You can either use the menu 'File' and 'Open'

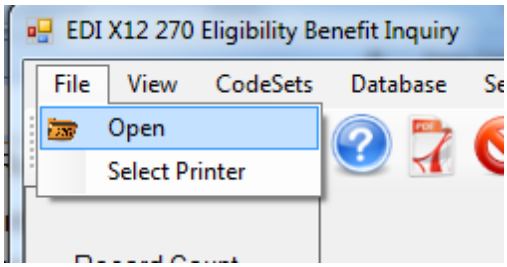
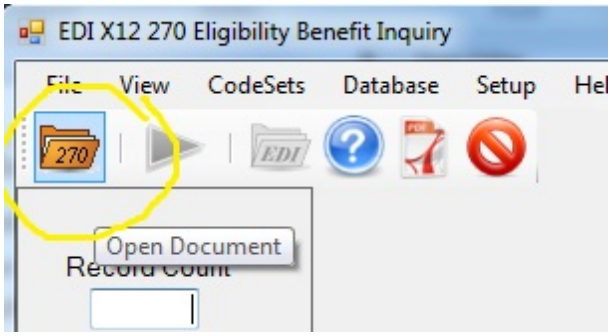


Figure1: Opening a file through the menu

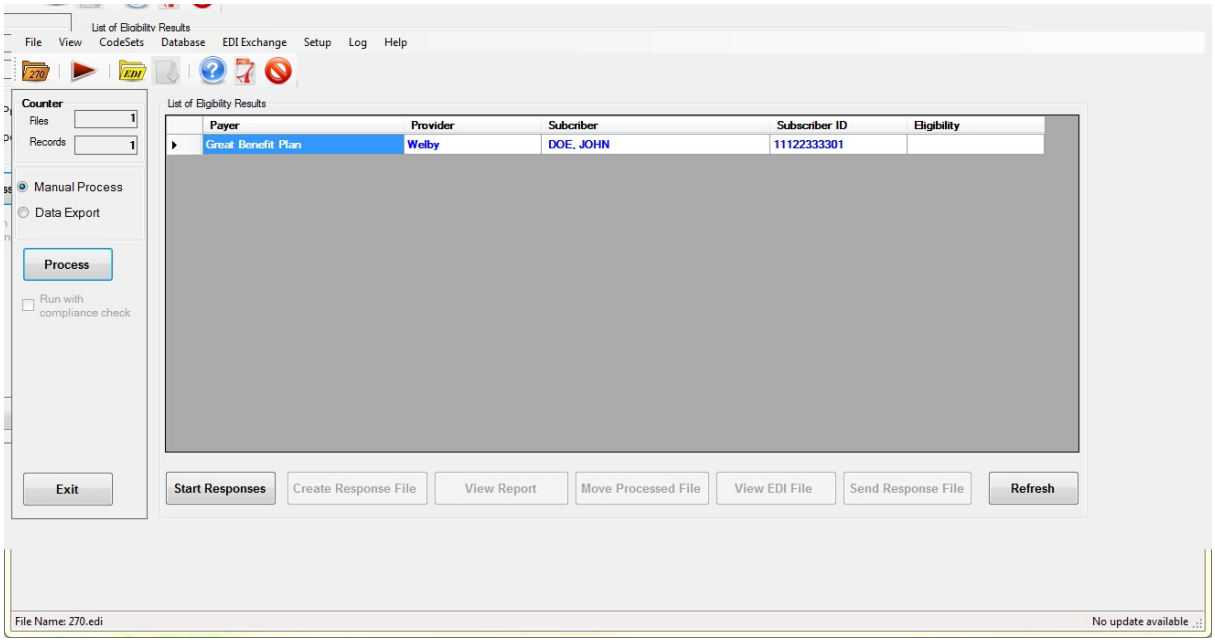
or the taskbar icon the 'Open 270 Folder' icon to bring up the Windows File Chooser



The 'File Open' task bar icon

Navigate to your 270 EDI file and select it.

Now you can click on the red arrow button or on the 'Process' button and you will see the listing of individual requests in the request grid.



After parsing a 270 request file

We can see that this particular 270 file contained 3 different requests. The window lists the payer, the provider and the subscriber and ID. Please note that the last column with the eligibility information is empty.

We can either double-click on a row in the request grid or by clicking on the 'Start Responses' button. The 'Start Responses' button will start with request number one.

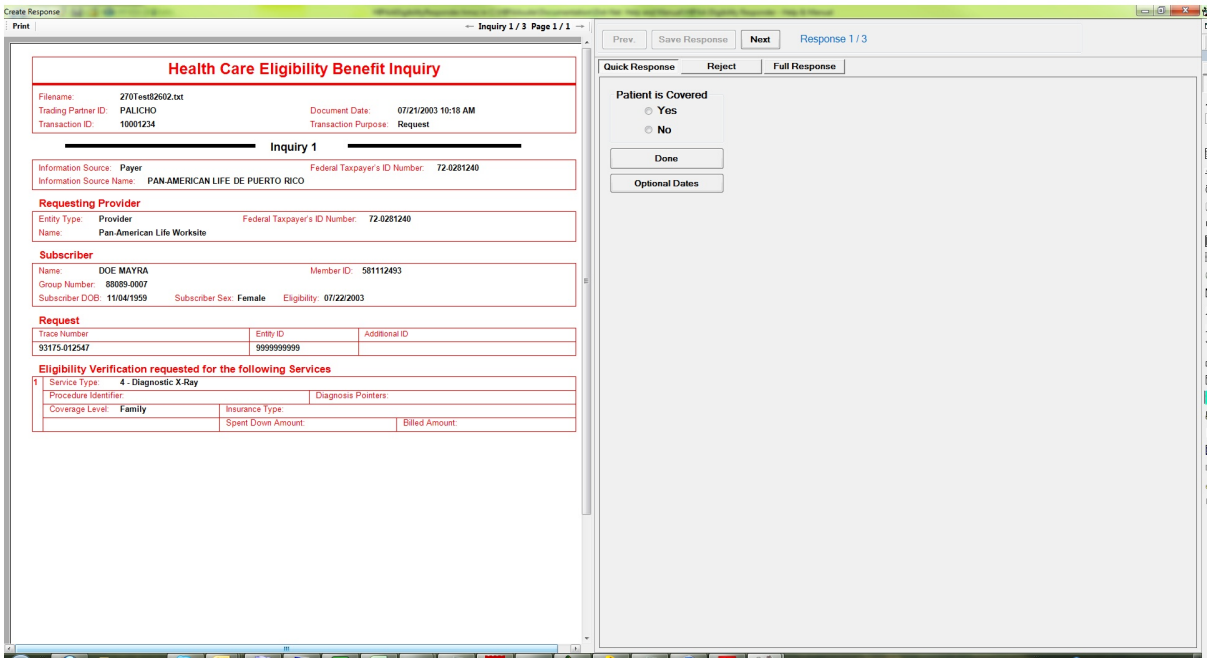
Once the eligibility information has been added, one can create the response file by clicking on the 'Create Response File' button. Once the file has been created the 'View EDI File' and the 'View Report' button will be enabled

The 'Move Processed File' button will move the file to the directory that has been specified in the setup screen.

4.3 Answering an individual Request

When we double-click a line in the request grid or click the 'Start Response' button, the following split screen will come up that lists, in detail, all the information contained in the request on the left side and has the tools to create the answer on the right. Since the

incoming data cannot be changed, is makes sense to display the request in a report form and visually separating the request from the response.



The detailed view of an eligibility request on the left and the response creation on the left

Here one can see the details of the request starting with envelope data, the organization that has the desired information, the requesting provider with all his information is below, followed by subscriber information as well as dependent information if the patient is not the subscriber.The details of request are then displayed in the grid below. This particular request has 1 request line

The response option and the navigation within the file.

We have several options to answer this request

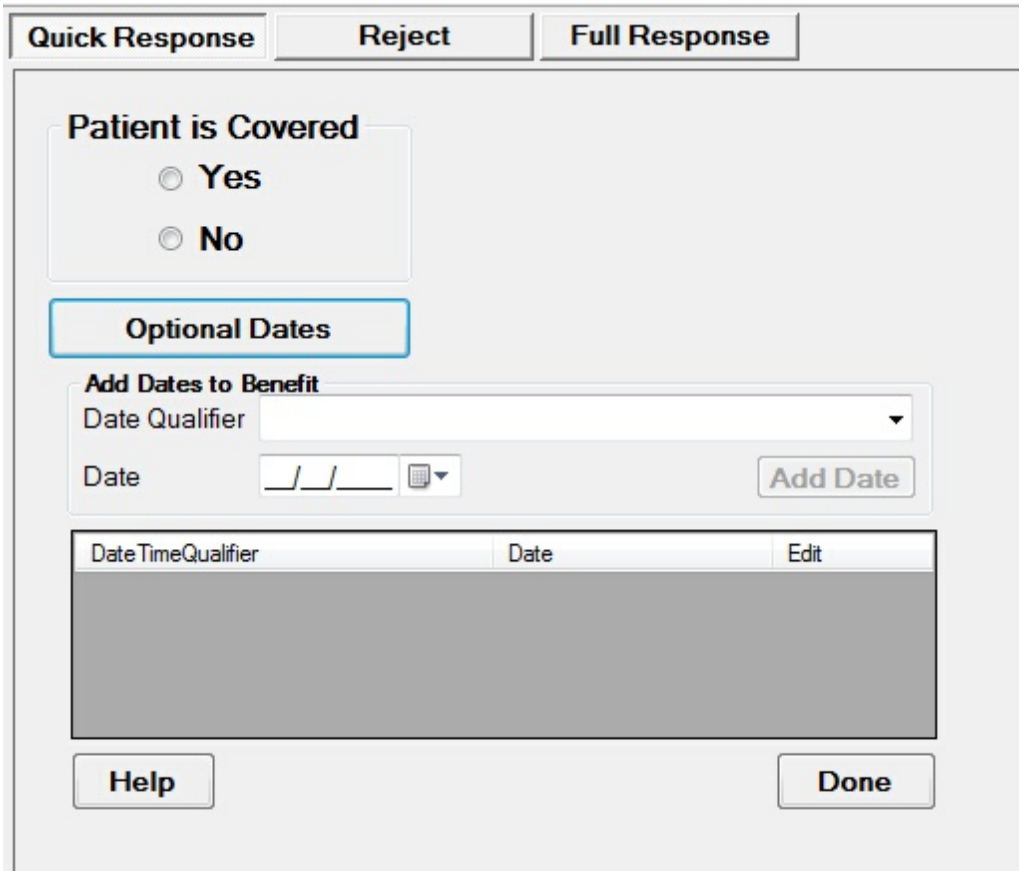
1. Give a quick response with the HIPAA minimum information
2. Reject the request for a variety of reasons
3. Give a full response with all the capability of the 271 transaction set.

4.4 Returning the Minimum Information

According to the implementation guide it is acceptable to just return whether a subscriber is eligible for benefits at the time of the request or not.

If this is all you want to return to the requester, click on the 'Quick Response' button.

You will see the Response: Minimum Response screen:



The HIPAA Minimum Response screen

Dates are optional in the Quick Response Mode

Here you can choose from a variety of different date types from the drop down menu and select the date as well.

Date types that you can choose from are:

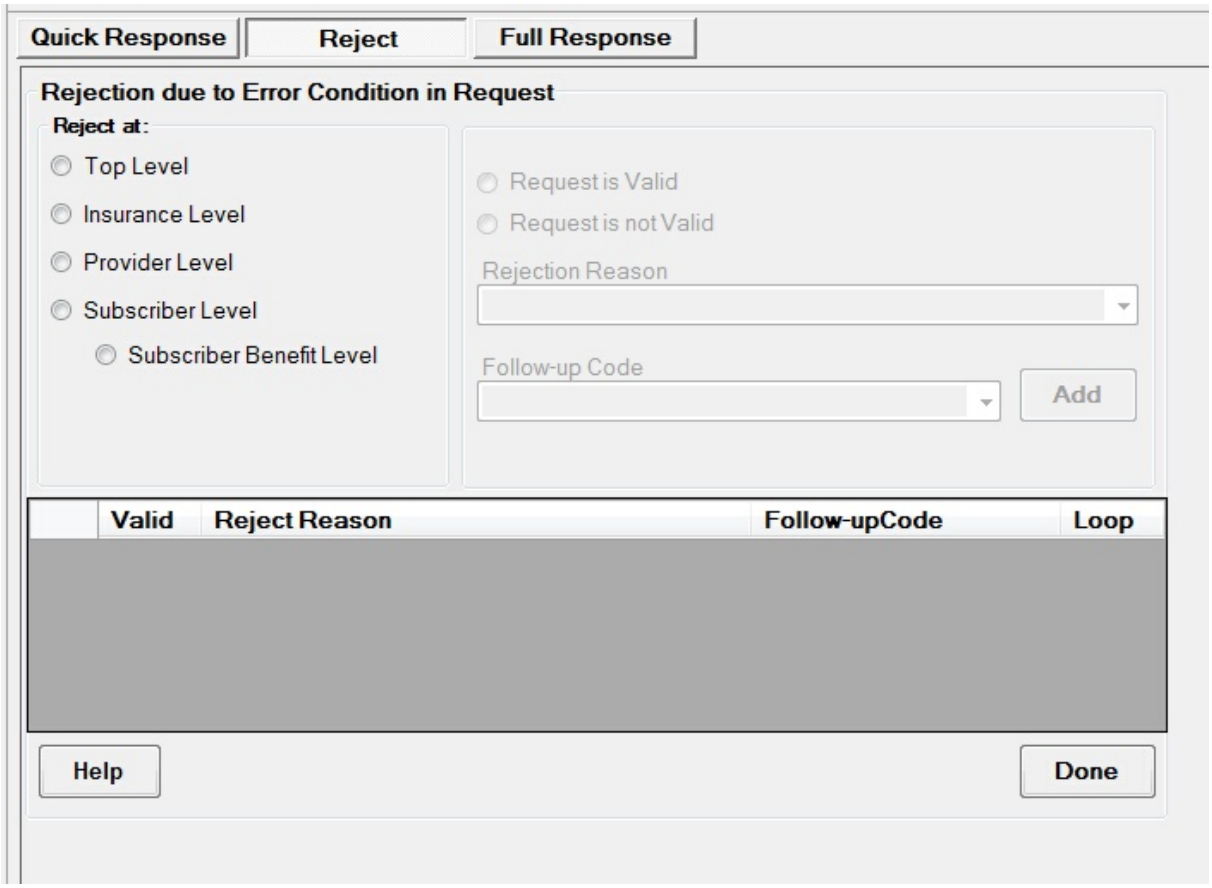
193 Period Start
194 Period End
198 Completion
290 Coordination of Benefits
292 Benefit
295 Primary Care Provider
304 Latest Visit or Consultation
307 Eligibility
318 Added
348 Benefit Begin
349 Benefit End
356 Eligibility Begin
357 Eligibility End
435 Admission
472 Service
636 Date of Last Update

Once you are done, click the 'Done' button and return to the detailed request screen.

You can now save your eligibility information.

4.5 Rejecting a Request

When you click the 'Reject' button you will be confronted with the Response: Reject Eligibility Benefit Inquiry screen:



The Reject screen

You can see in the left upper part of the screen an options menu. Here you have to choose at which level the request is to be rejected. Accordingly, the Reject Reasons will be available. Each level has different reject reasons. The most likely reason to reject is that the provider is not in the network or the subscriber/patient is not on file.

- **Top Level**:Required when the request could not be processed at a system or application level based on the entities identified in ISA06, ISA08, GS02 or GS03 and to indicate what action the originator of the request transaction should take. Below are valid reject reasons for Top level rejections

  04 Authorized Quantity Exceeded

  41 Authorization/Access Restrictions

  42 Unable to Respond at Current Time

79 Invalid Participant Identification

- **Insurance Level**:Required when the request could not be processed at a system or application level when specifically related to the information source data contained in the original 270 transaction's information source name loop (Loop 2100A). it also indicates that the information source itself is experiencing system problems and to indicate what action the originator of the request transaction should take. Below are the valid reject reasons for an insurance level rejection

  04 Authorized Quantity Exceeded

  41 Authorization/Access Restrictions

  42 Unable to Respond at Current Time

  79 Invalid Participant Identification

  80 No Response received - Transaction Terminated

  T4 Payer Name or Identifier Missing

- **Provider Level:**Required when the request could not be processed at a system or application level when specifically related to the information receiver data contained in the original 270 transaction's information receiver name loop (Loop 2100B) and to indicate what action the originator of the request transaction should take. Below are the valid reject reasons for an provider level rejection

  15 Required application data missing

  41 Authorization/Access Restrictions

  43 Invalid/Missing Provider Identification

  44 Invalid/Missing Provider Name

  45 Invalid/Missing Provider Specialty

  46 Invalid/Missing Provider Phone Number

  47 Invalid/Missing Provider State

  48 Invalid/Missing Referring Provider Identification Number

  50 Provider Ineligible for Inquiries

  51 Provider Not on File

79 Invalid Participant Identification

97 Invalid or Missing Provider Address

T4 Payer Name or Identifier Missing

- **Subscriber or Dependent Level**: Required when the request could not be processed at a system or application level when specifically related to the data contained in the original 270 transaction's subscriber name loop (Loop 2100C) and to indicate what action the originator of the request transaction should take.

  15 Required application data missing

  35 Out of Network

  42 Unable to Respond at Current Time

  43 Invalid/Missing Provider Identification

  45 Invalid/Missing Provider Specialty

  47 Invalid/Missing Provider State

  48 Invalid/Missing Referring Provider Identification Number

  49 Provider is Not Primary Care Physician

  51 Provider Not on File

  52 Service Dates Not Within Provider Plan Enrollment

  56 Inappropriate Date

  57 Invalid/Missing Date(s) of Service

  58 Invalid/Missing Date-of-Birth

  60 Date of Birth Follows Date(s) of Service

  61 Date of Death Precedes Date(s) of Service

  62 Date of Service Not Within Allowable Inquiry Period

  63 Date of Service in Future

  71 Patient Birth Date Does Not Match That for the Patient on the Database

  72 Invalid/Missing Subscriber/Insured ID

73 Invalid/Missing Subscriber/Insured Name

74 Invalid/Missing Subscriber/Insured Gender Code

75 Subscriber/Insured Not Found

76 Duplicate Subscriber/Insured ID Number

78 Subscriber/Insured Not in Group/Plan Identified

- **Subscriber or Dependent Benefit Level**: Required when the request could not be processed at a system or application level when specifically related to the data contained in the original 270 transaction's dependent name loop (Loop 2100D) and to indicate what action the originator of the request transaction should take.

  15 Required application data missing

  35 Out of Network

  42 Unable to Respond at Current Time

  43 Invalid/Missing Provider Identification

  45 Invalid/Missing Provider Specialty

  47 Invalid/Missing Provider State

  48 Invalid/Missing Referring Provider Identification Number

  49 Provider is Not Primary Care Physician

  51 Provider Not on File

  52 Service Dates Not Within Provider Plan Enrollment

  56 Inappropriate Date

  57 Invalid/Missing Date(s) of Service

  58 Invalid/Missing Date-of-Birth

  60 Date of Birth Follows Date(s) of Service

  61 Date of Death Precedes Date(s) of Service

  62 Date of Service Not Within Allowable Inquiry Period

  63 Date of Service in Future

64 Invalid/Missing Patient ID

65 Invalid/Missing Patient Name

66 Invalid/Missing Patient Gender Code

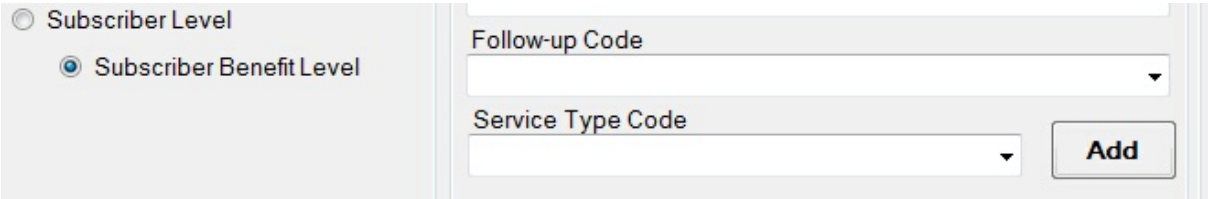
67 Patient Not Found

68 Duplicate Patient ID Number

71 Patient Birth Date Does Not Match That for the Patient on the Database

77 Subscriber Found, Patient Not Found

When you select Subscriber or Patient Benefit Level, drop down box appears that lets you select which benefit line is rejected.



The drop-down box that let's you choose the benefit line of the request.

According to the reject reason select a meaningful follow-up code. There are:

C Please Correct and Resubmit

N Resubmission Not Allowed

R Resubmission Allowed (Use only when AAA03 is “42".)

S Do Not Resubmit; Inquiry Initiated to a Third Party

W Please Wait 30 Days and Resubmit

X Please Wait 10 Days and Resubmit

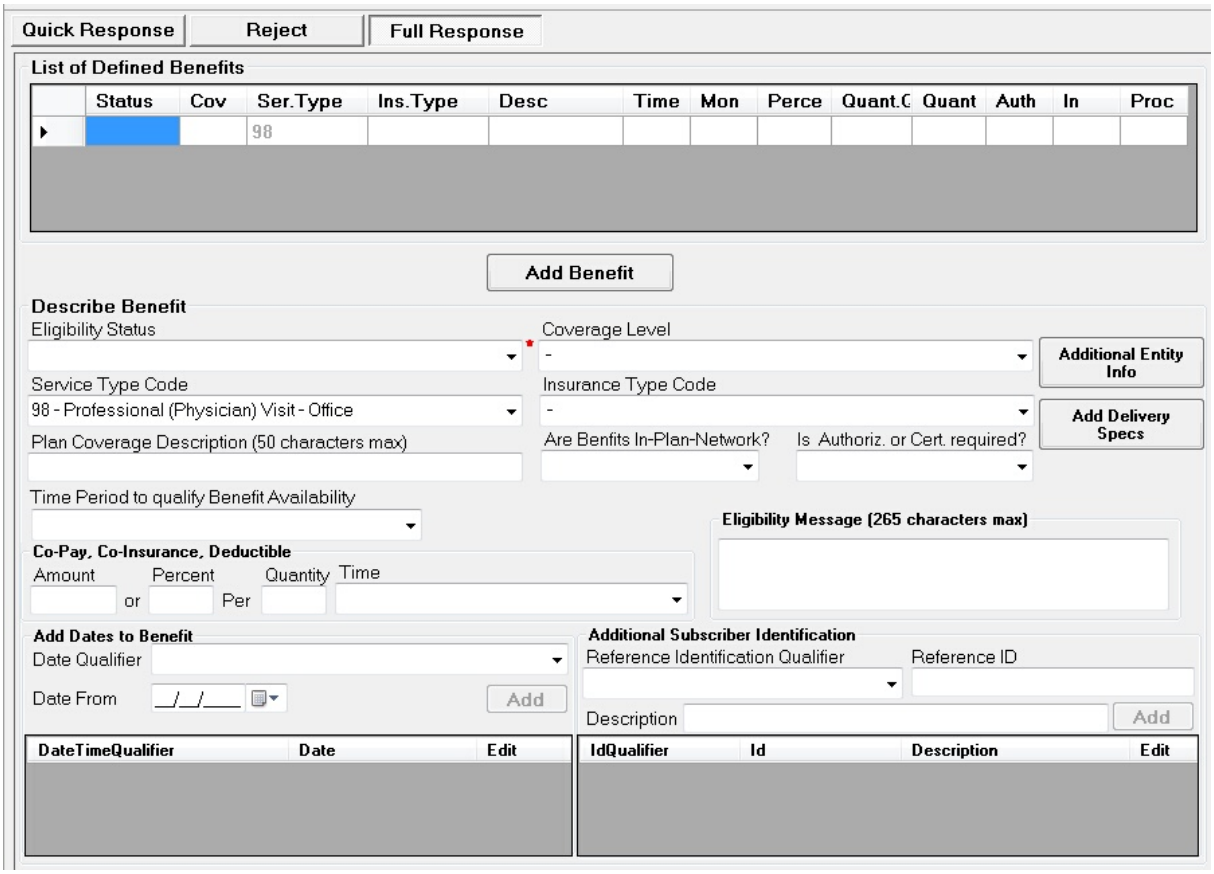
Y Do Not Resubmit; We Will Hold Your Request and Respond Again Shortly (Use only when AAA03 is “42".)

Once you are done, click on the 'Save' button and return to the request screen.

4.6 Creating a Full Response

4.6.1 Eligibility and Benefit Information

If you choose to create a full response, you will see the **Response: Eligibility and Benefit Information** screen:



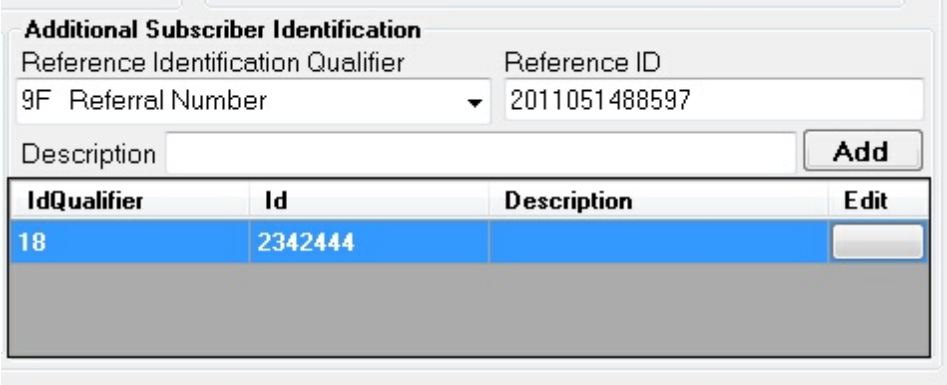
The Eligibility and Benefit screen

When you first call up this screen, you will notice that some values in the drop down boxes are already filled in. This information is carried over from the request. While the implementation guide does not force you to return the specifically requested information, the HIPAA Eligibility Responder defaults to the requested information. While creating benefit information, you can either leave the selected info and answer the request or select any other values. If the request is for multiple services, that means there are several lines in the request screen, you will see for each new benefit that you

define the default information pre-selected.

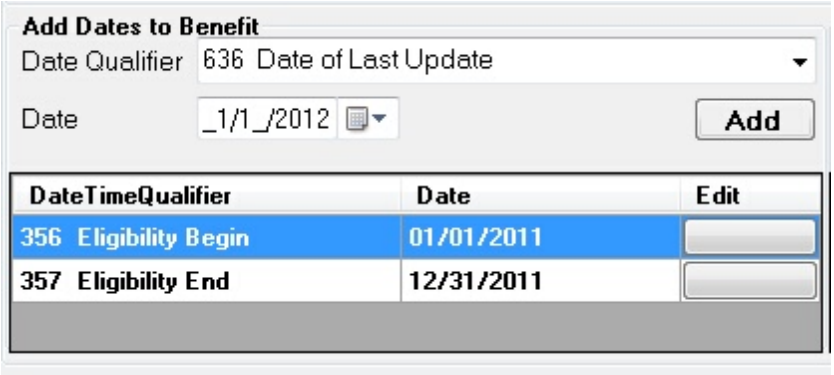
Fill in all the information that you have on the patient. If you have further information in regard to the benefit such as dates and ID's you can add this information in the bottom of the form. This way the additional information is clearly belonging to the current benefit.

You can add insurance information such as policy numbers, employee number etc. to the benefit information. This information will be transmitted in the 'REF' segments.



Adding Identifiers to the Benefit

You might want to specify time periods that pertains to the benefit. You can do this on the bottom of the screen



The Date screen

Here you can choose from a variety of different date types from the drop down menu and select the date as well.

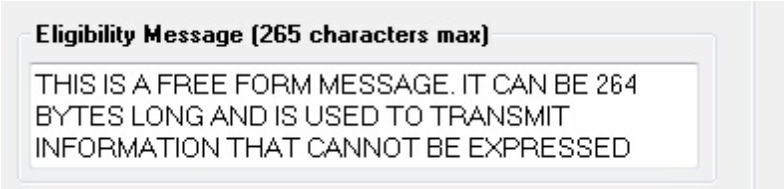
Date types that you can choose from are:

193 Period Start
194 Period End
198 Completion
290 Coordination of Benefits
292 Benefit
295 Primary Care Provider
304 Latest Visit or Consultation
307 Eligibility
318 Added
348 Benefit Begin
349 Benefit End
356 Eligibility Begin
357 Eligibility End
435 Admission
472 Service
636 Date of Last Update

The above screen shows you a sample with three additional Identifiers and a description for one of them.

Choose a qualifier and an Id. The description is optional. When you click the save button, the additional identifier will be saved.

The last segment narrowing the benefit information is the 'MSG' segment. This segment an contain any text up to 256 characters long that can describe a benefit or have any other information that might be important and can only be expressed in free format.



The free form Message

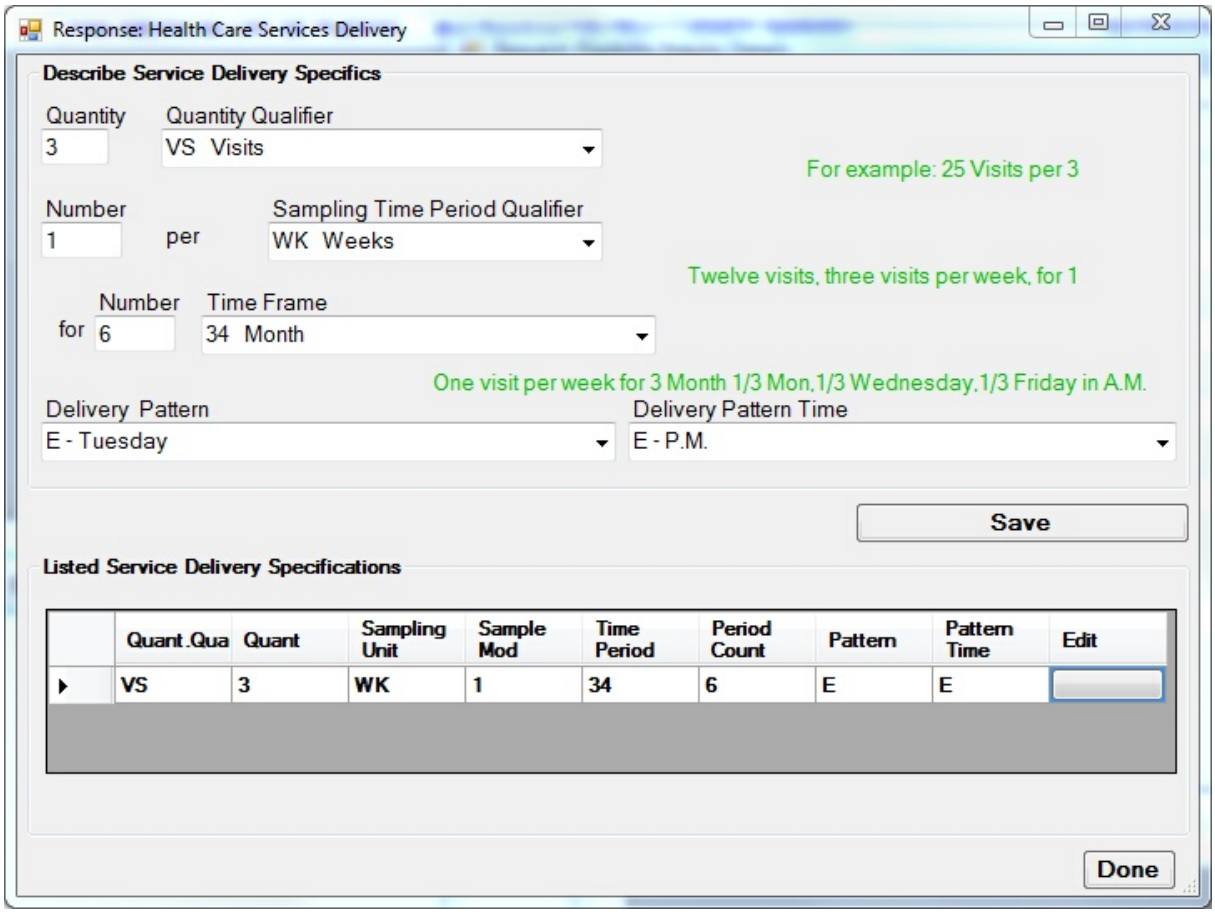
Once you are done with a benefit, you can click on 'Add Benefit' and the line is saved to the benefit grid.

If you want to go back and edit a benefit or add additional information, just double click a line in the defined benefit grid and the data is back in the fields and drop down boxes above, ready to be added. You will see that the 'Add Benefit' button reads now 'Save Benefit' This way you know that you are in edit mode. After you made your changes or added information, click on 'Save Benefit' to update the response.

4.6.2 Delivery Specific Infomation

In some cases it might be advantageous to narrow the eligibility information with delivery specification. The 271 transaction set has therefore the 'HSD' (Health Service Delivery) segment.

The HIPAA Eligibility Responder has a screen for this information. If you click in the benefit screen on the 'Add Delivery Specs' button, you will see the **Response: Health Care Services Delivery** screen:



The Health care Service Delivery screen

The information is a bit difficult to put in. Therefore we added some samples in green onto the form to give you an idea what kind of information this screen takes.

For example a physical therapy benefit could specify how many session within a given time frame are covered, or hospice service that consists of home visits could be specified how many times a nurse would come.

The above figure shows the three delivery specification as mentioned in the green print.

4.6.3 Adding Entity Information

The 271 transaction set has a provision to add so called 'entity' information to the response. Entities could be

- Primary Care Physician
- Another Payer
- A legal Representative

and a few others.

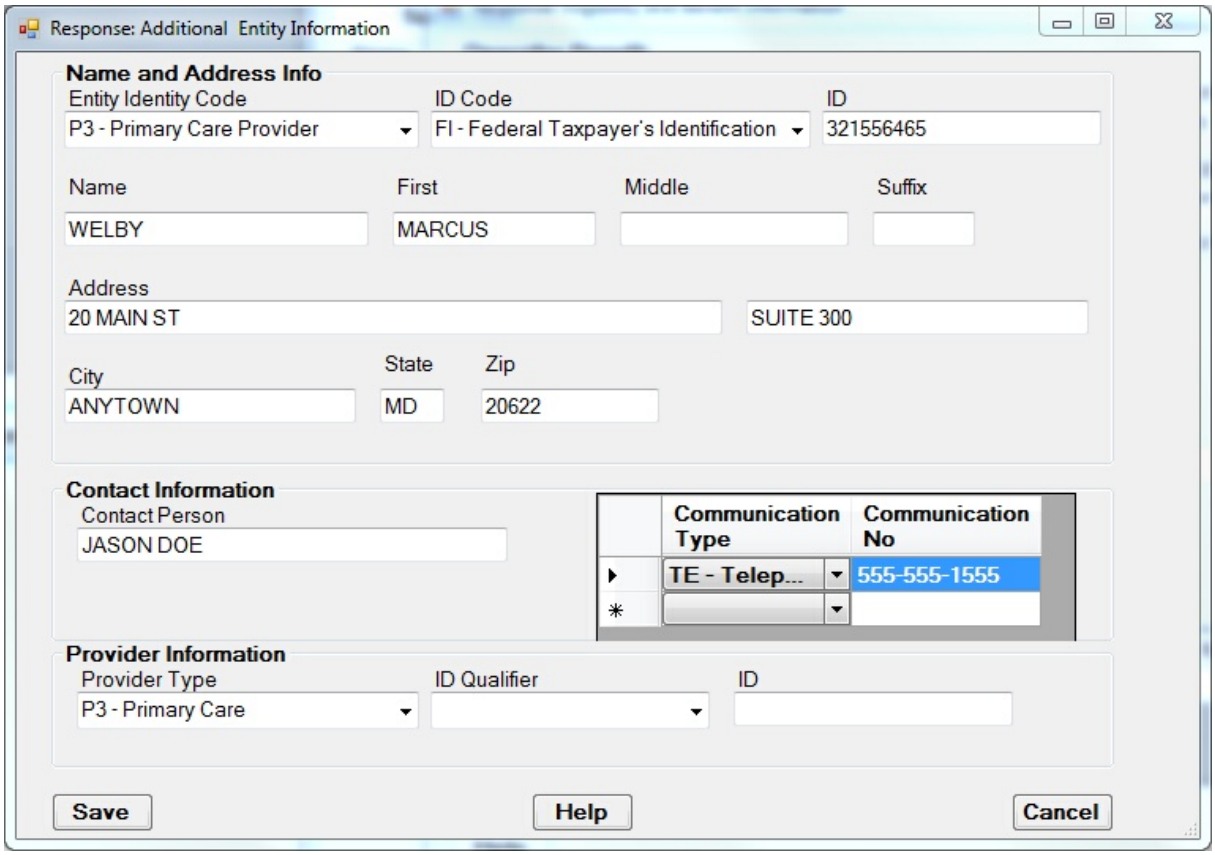
Required when provider was identified by Identification Number (not Taxonomy Code) in the 270 Inquiry and was used in the determination of the eligibility or benefit response;

or

Required when needed to identify an entity associated with the eligibility or benefits being identified in the 2110D loop such as a provider (e.g. primary care provider), an individual, an organization, another payer, or another information source;

If not required by this implementation guide, do not send.

The Response: Eligibility and Benefit Information screen has the 'Add Provider Info' button. Click this to bring up the 'Response: Additional Entity Information screen



The Additional Entity Information screen

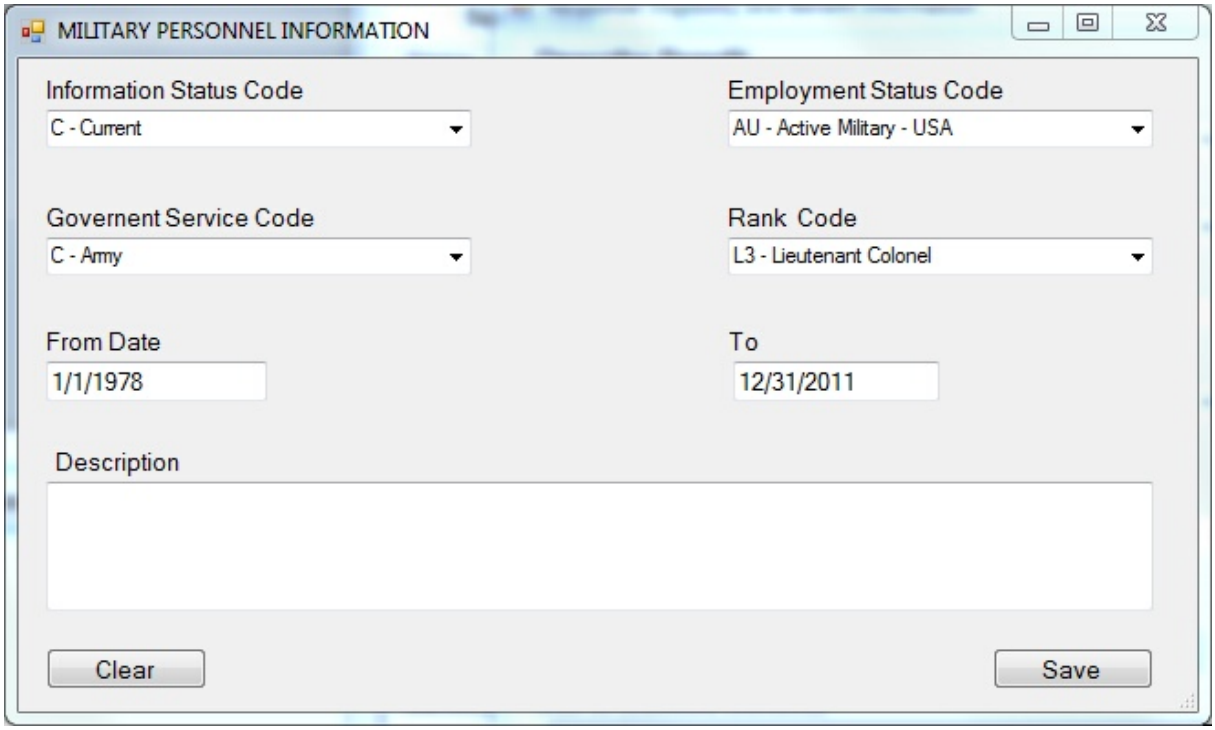
Adding the information does not need further explanation.

4.6.4 Military Personell Information

The MPI segment that contains Military Personnel Information was introduced with 5010 standard.

This information is required when this transaction is processed by DOD or CHAMPUS/ TRICARE and when necessary to convey the Subscriber's military service.

Clicking on the Military Information button will bring up the following screen



The Military Personnel screen

4.7 Creating the Response file

Once you have added the eligibility information and you get back to the main screen, you will now see information in the eligibility column, the last column in the request grid.

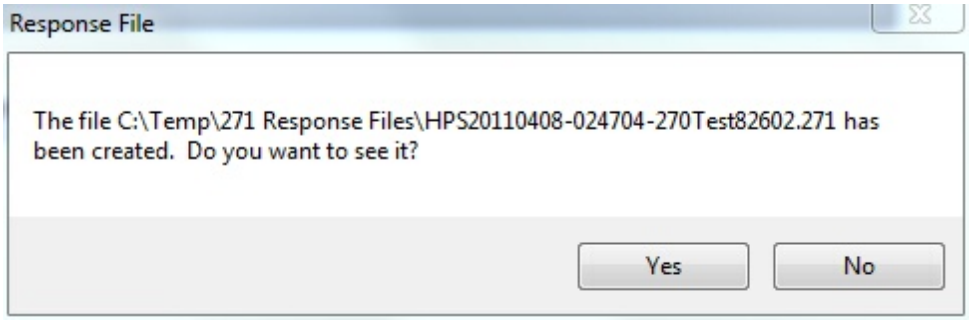
You are now ready to create the EDI response file.

Payer	Provider	Subcriber	Subscriber ID	Eligibility
PAN-AMERICAN LIFE DE PUERTO...	Pan-American Life Wor...	DOE, MAYRA	93175-012547	EB*1*FAM*4*C1***5**V...
PAN-AMERICAN LIFE DE PUERTO...	Pan-American Life Wor...	SMITH, MARISEL	93175-012548	
PAN-AMERICAN LIFE DE PUERTO...	Pan-American Life Wor...	JONES, MARISEL	93175-012549	

You can see now that eligibility information has been added in the last column

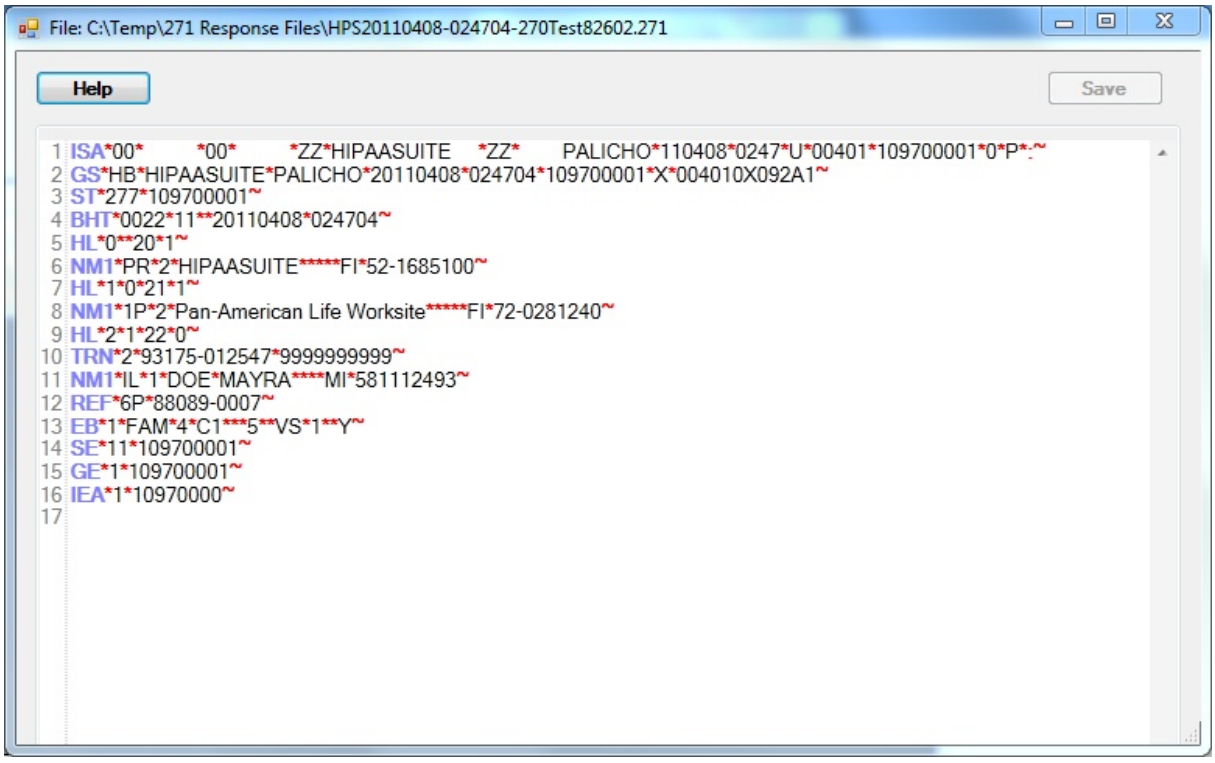
Click on the 'Create Response File' button and the 271 file will be created and written into the out directory that you specified during system setup.

Once the file has been created, a message box appears, informing you that the file has been created and asking you if you want to see the file.



The message after creating a 271 response

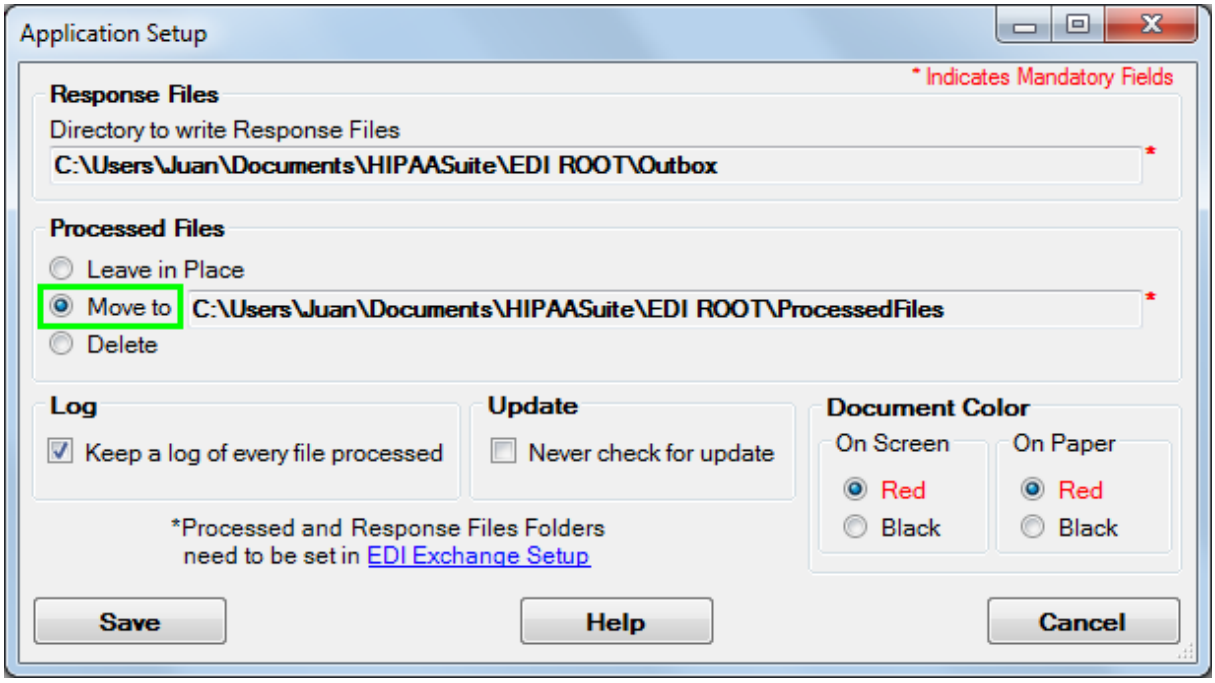
If you click yes and if you have the EDI File Editor installed and mapped, the File Editor will come up and display your file.



The Response File

4.8 Moving the Processed File

Once you have responded to a 270 eligibility request, you might want to archive the file and take it out of the way to prevent duplicate processing. If you have specified a directory for processed files in the setup and checked the '*Move to*' option, the file will be moved after processing.



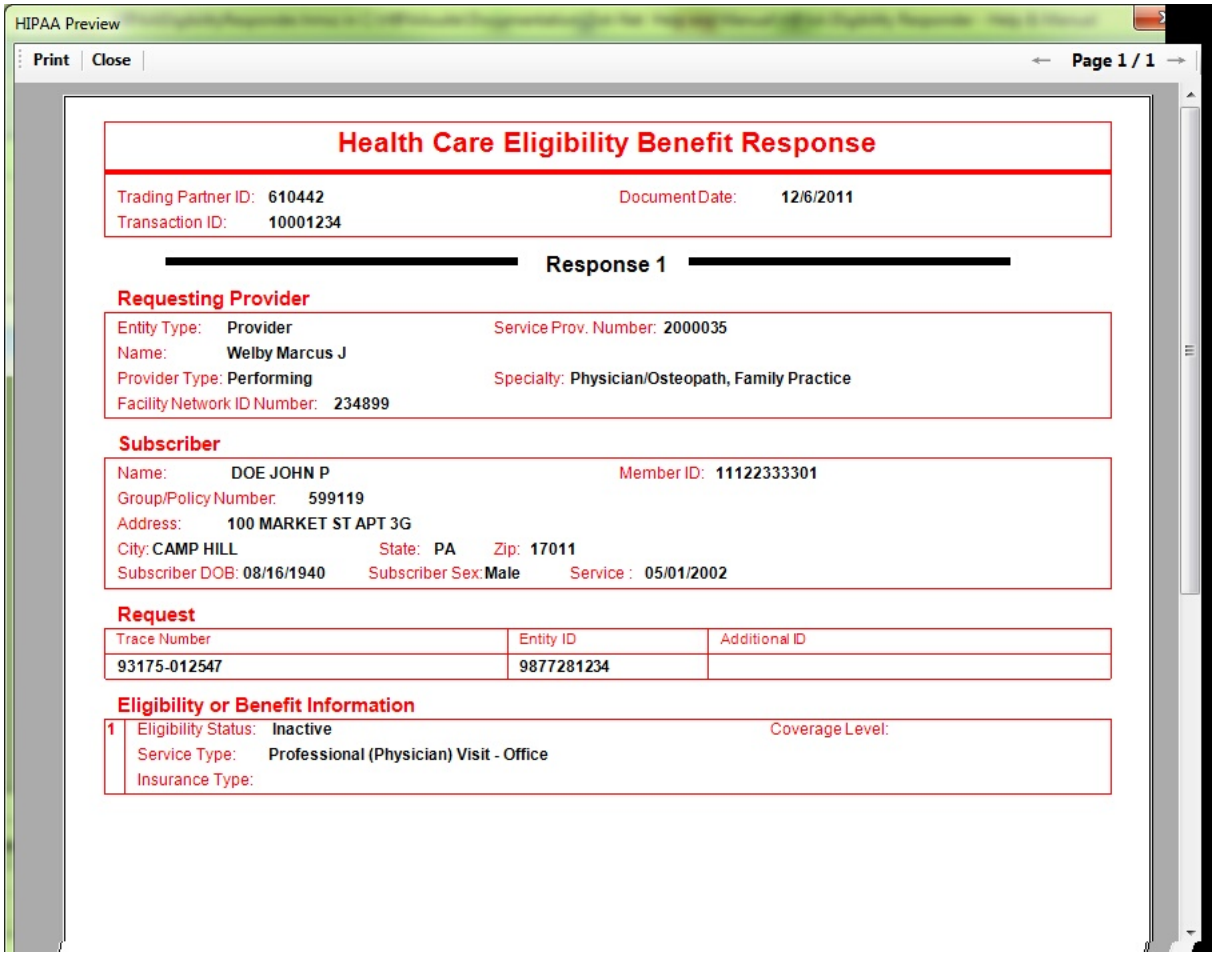
This option moves the file after processing to keep the EDI root directory tidy.

4.9 Viewing the Response

After creating the response and writing it to file you can click the button "View Report" This functionality will display the 271 transaction that you just created in a report type.

The "View Report" button

Pressing it will bring up the report



The response as a report.

5 Database Interaction

5.1 Introduction

The HIPAA Eligibility Responder has a database interface that allows the export of the EDI request data in an SQL compliant database such as Microsoft SQL Server, mySQL, Access or Oracle. The data is placed in two hierarchical tables,

- EDI_EligibilityHeader and
- EDI_EligibilityDetail.

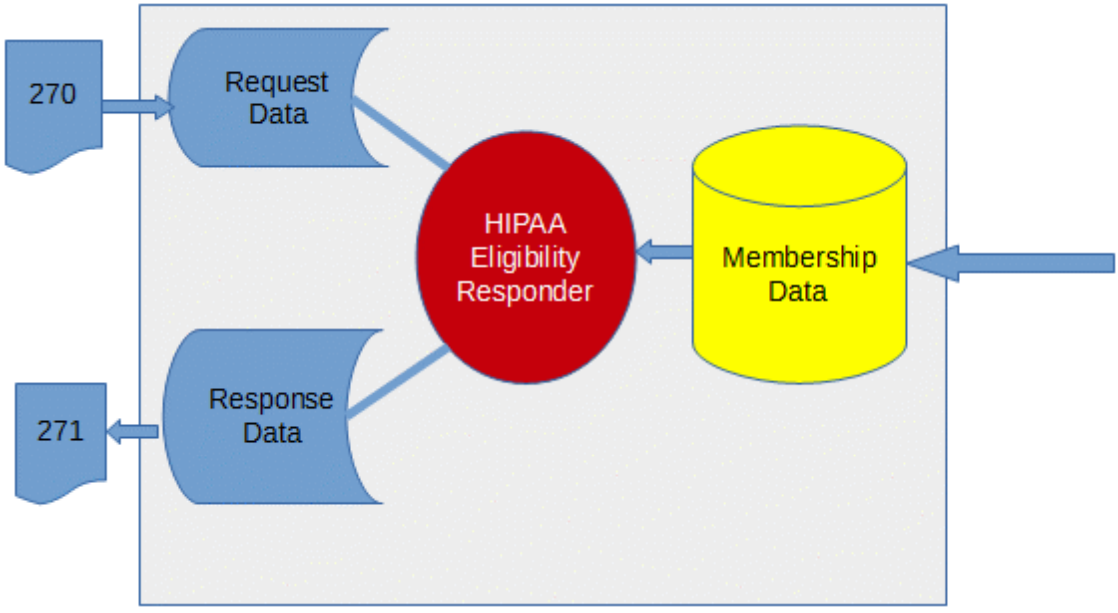
In addition the response can be saved. Here we use a schema of 4 tables.

- EDI_ResponseHeader which contains file level information
- EDI_ResponseMember which contains demographic and other member related information
- EDI_ResponseBenefits which contains benefit information, in a one-to-many relationship, meaning that a member record can have multiple benefit records associated
- EDI_EligRequestValidation which contains error messages in case the response was a rejection

Lastly there are the tables that contain membership information that will be used to create automatic responses. These tables

- EDI_CoveredMembers and
- EDI_CoveredBenefits

are there to be populated by the users with their healthplan's data. This process will require custom programming either on the side of the user or contracted out to HIPAAsuite.



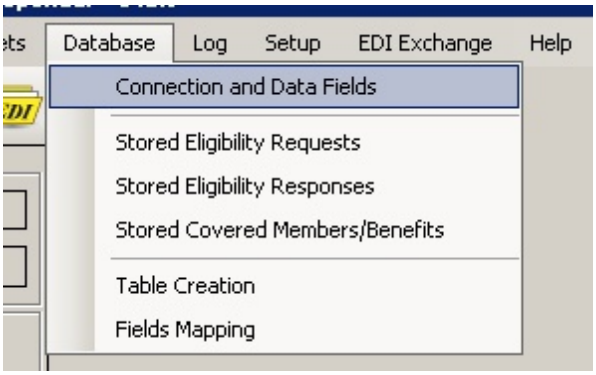
Schematics of the database design for the HIPAA Eligibility Responder

There are scripts provided and a screen to generate those tables for a few important databases such as Microsoft SQL Server, the open-source database mySQL and Oracle.

The tables contain nearly every possible element of the request and it is possible to answer requests from the database.

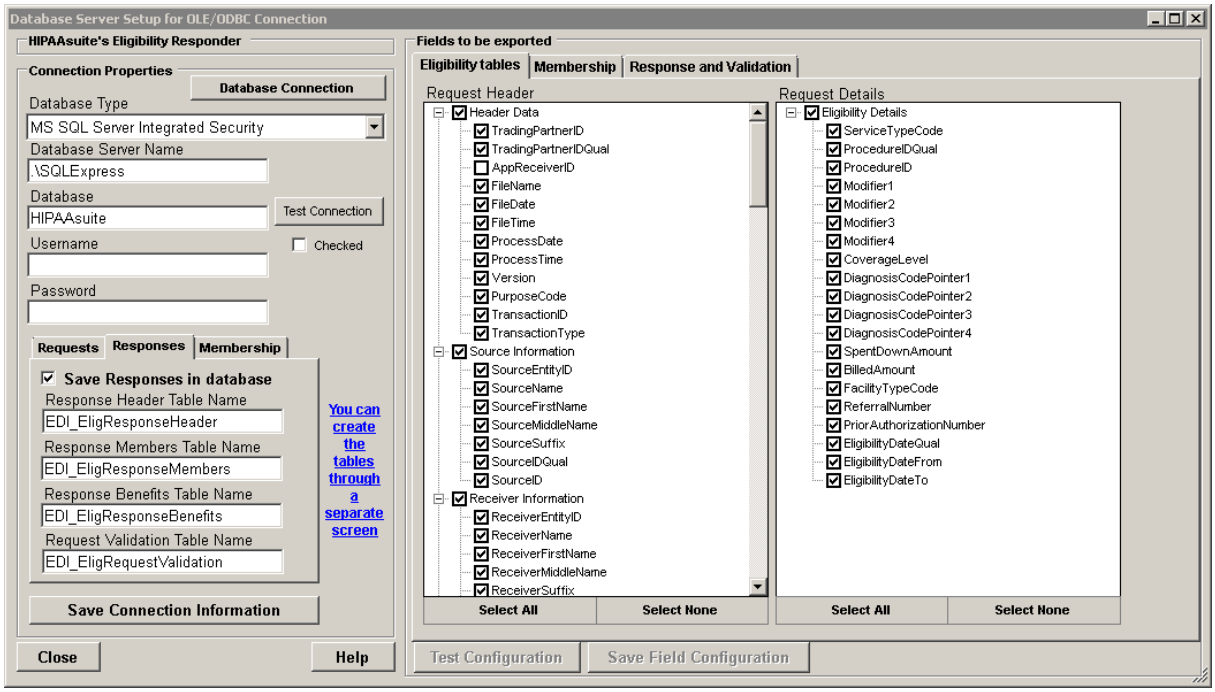
5.2 Database Setup

Under the main menu item 'Database' is the first option "Connection and Data Fields"



The menu under 'Database'

When you click on it the following screen comes up



Database connection and data fields

On the left side of the screen you see the connection setup, here again in detail

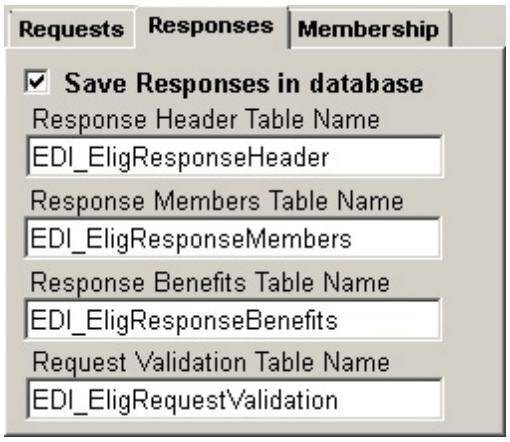
Defining the connection parameters. Note that this image shows the check mark at "Save Responses in database"

- Database Type --- is either ODBC or Microsoft SQL Server either with Windows Authentication or with explicit credentials (If you need other types, please contact us for customizations)
- Database Server Name or DSN --- In case of SQL server this is the IP address or the name of the database server, for ODBC this is the Data Source Name (DSN) that is defined through the ODBC setup in the Control Panel of Windows
- Database --- This is the database under the above connection, usually not needed in ODBC setup.
- Username --- A defined user that has privileges to the database, usually not needed in ODBC setup
- Password --- Usually not needed in ODBC setup.
- Eligibility Request Header Table Name --- The name that you give to your Eligibility header table. A default name is suggested but can be changed

- Eligibility Request Detail Table Name --- The name of the table that contains the line information. A default name is suggested but can be changed
- Eligibility Response Header table name -- This box shows up if you choose to save the response information
- Eligibility Response Member table name
- Eligibility Response Benefit table name
- Eligibility Request Validation table name
- Covered Members table name
- Covered Benefits table name

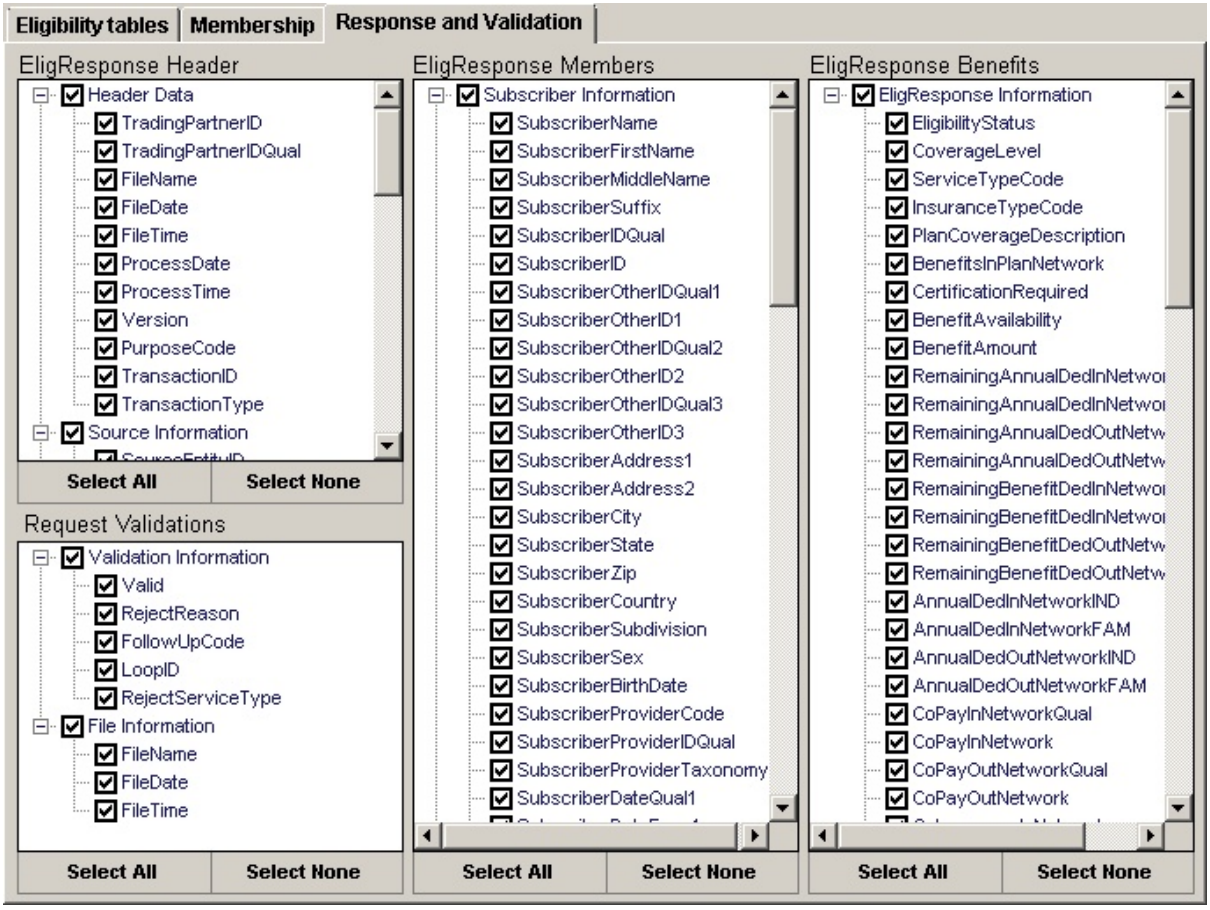
You can create the tables through a separate screen with scripts available in many database flavors

If you select to save the responses in the database, you will see 4 more text fields appear



Checking to save responses reveals 4 more tables

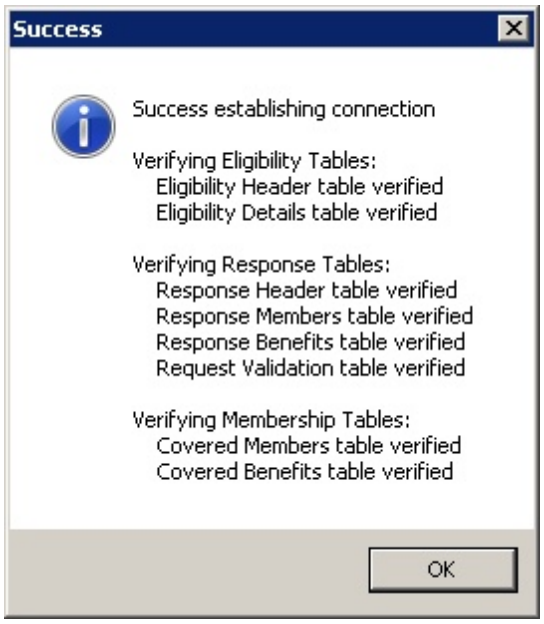
These four tables are used to store the responses created.



The tab with the fields of the response tables

After filling in all the information, save the information and test the connection by clicking on the "Test Connection" button.

After establishing a connection and the existence of your tables is verified you will see a message



The success message that the connection works and that all tables have been verified

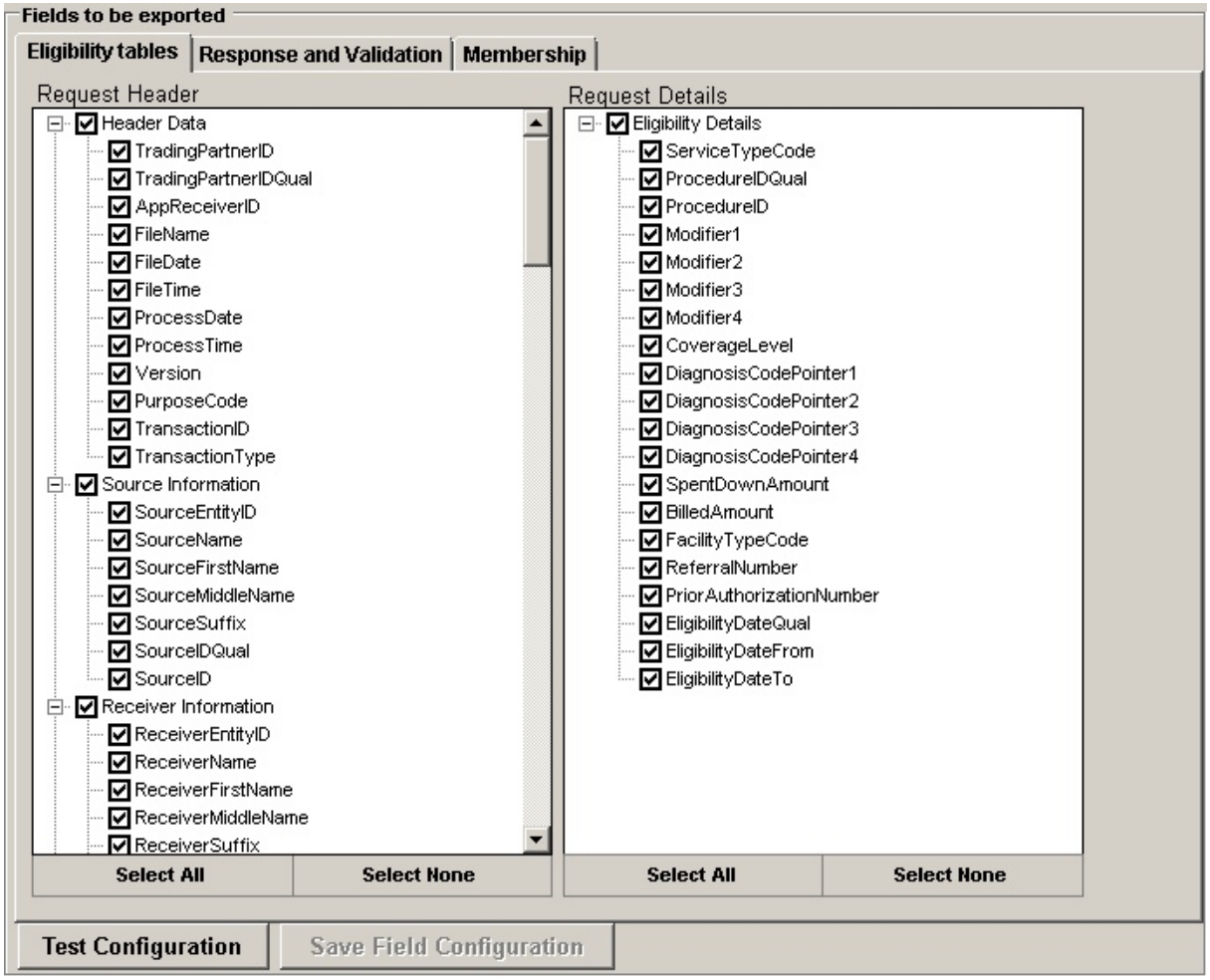
You cannot export eligibility requests before this connection tests successfully.

5.3 Field selection

The field selection part of this form lists all the fields that the program works with internally. They usually represent all the fields that can be in the EDI file. We recommend to select all fields. But if you are an expert and know that there are fields you will never use, you can deselect them and even remove them from the tables to obtain faster performance for example.

When you first bring up this screen, all the fields are deselected. You can click on the "Select All" button to check them all. Please do that for all 3 tabs and 8 tables.

You need to test the configuration first before you can save it. This will avoid later errors.



selecting the fields to be exported

If you have errors with individual fields checking out, a screen comes up that lists the fields in error and allows you to deselect them.

5.4 Renaming Fields

You can rename the fields listed for selection. The long field names that the HIPAA Premium Payment Master uses for the data export might be too long for some databases. IBM AS400, Clipper and other legacy databases cannot work with overly long filenames.

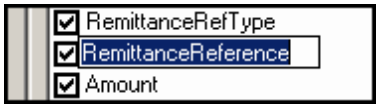
For this reason you can change the filenames to any name that you wish, as long as there are **no blank spaces** in the name.

The HIPAA Claim Master lets you change the names of the columns that you select for export. All you have to do is

1. Click twice the field name. Do not double-click, but click slowly twice. You will see that the field name is now editable.
2. Change the name to your value and leave the field by clicking somewhere else
3. Your field name has now been changed
4. Don't forget to save the new settings

Selecting a field

Click again, do not double click, on the label and you see that suddenly there is a frame around the name and the curser is placed at the end of the label. Now you can edit the label.

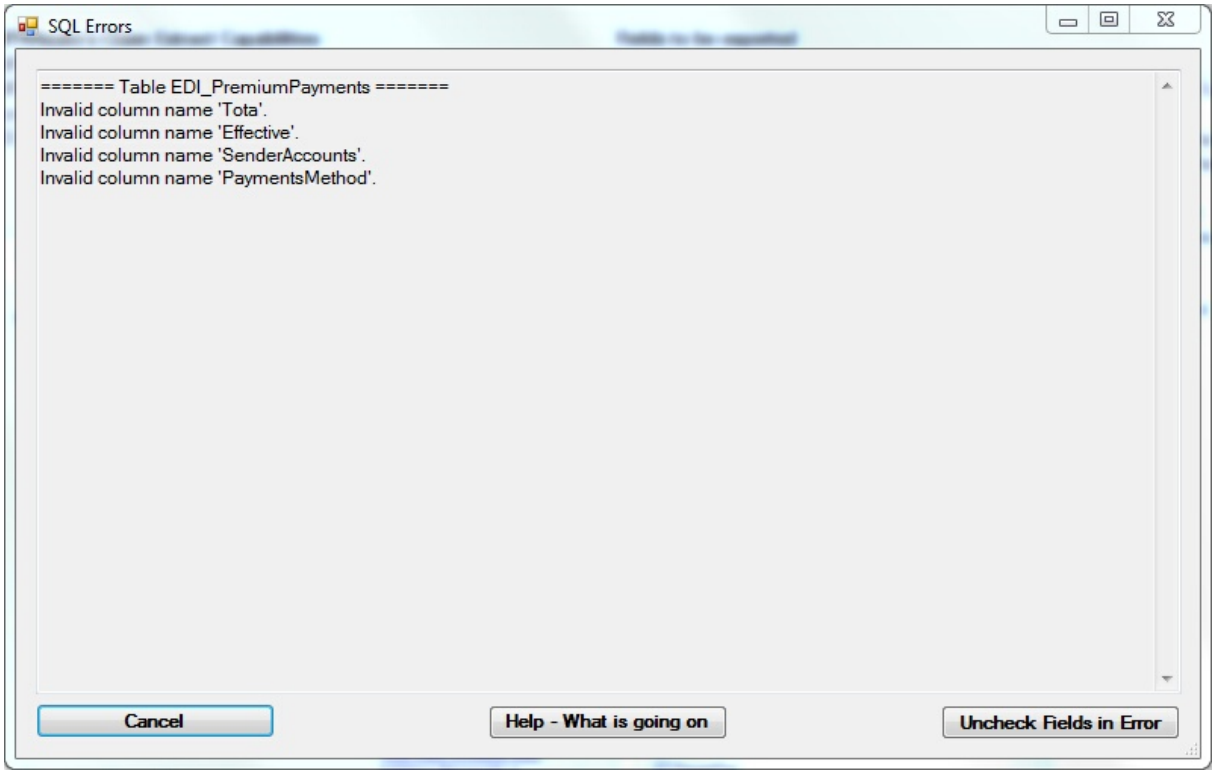


The field name in edit mode

The renamed field

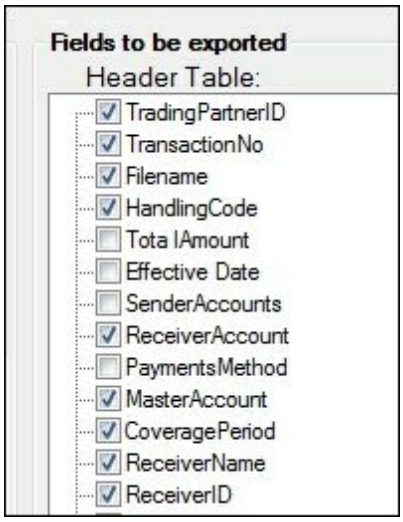
5.5 Field Errors

If fields don't exist in the database that you specified, you will see an error screen



The error screen you will see if the field selection contains non-existing fields.

Study the errors in detail and see what went wrong. In this case for demonstration purposes I changed a few names and of course that caused this error. My best option is to click the "Uncheck the Fields in Error" button and return to the field selection screen.



The fields in error are now unchecked.

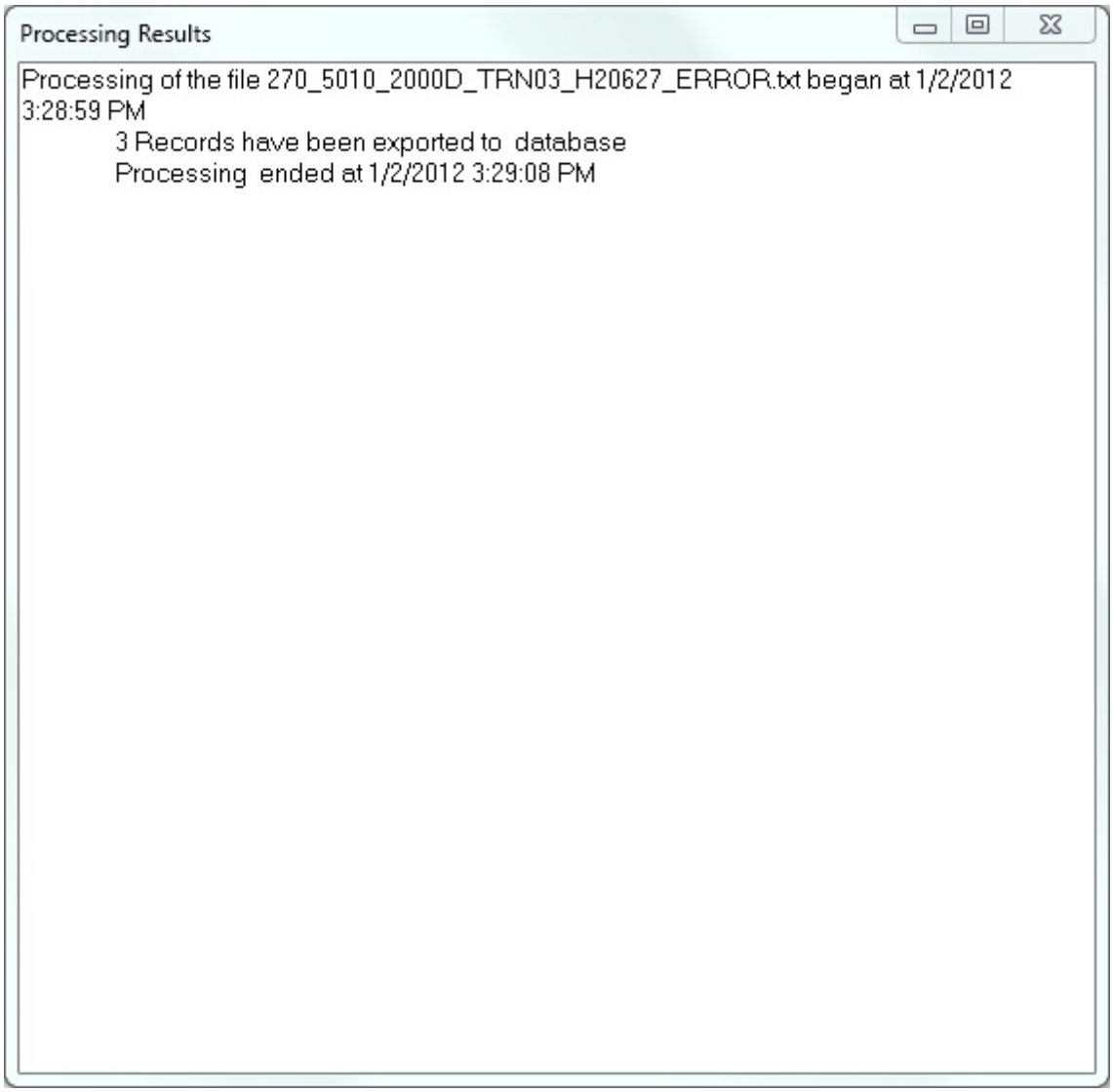
5.6 Exporting Eligibility Requests

Once the database connection and fields have been set up, you can export the data in the 270 EDI files to the database.

On the main screen, open a file and select 'Data Export'

Choosing data export and the counters

Then, when you process the file you will see the counters increasing and when the file is finished you will see a screen pop up with the processing results.



The screen with the process results.

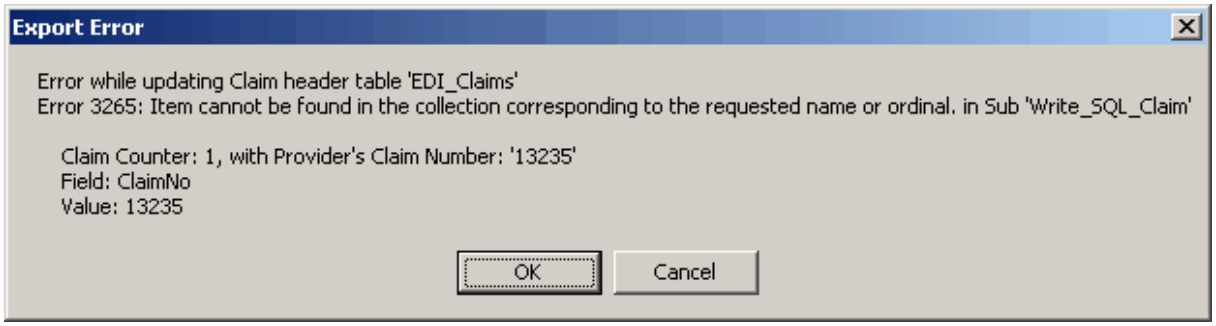
5.7 Database Errors

When you start exporting claims into the staging tables you might encounter errors at first. This usually results from table definition issues. The HIPAA Eligibility Responder displays a very detailed error message that tells you which claim failed, at what field and if applicable, which line.

This information should help you to trouble shoot the problems. It sometimes takes serious detective work to find and correct errors.

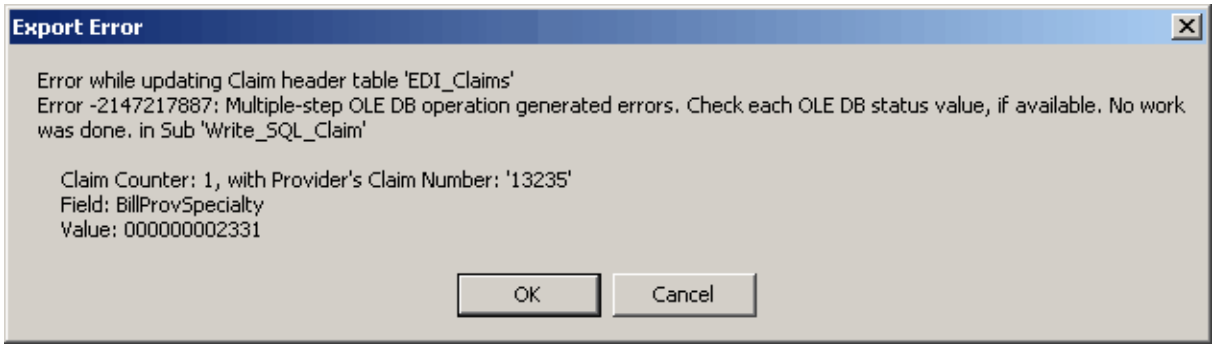
Below are some of the most common errors:

Item cannot be found:



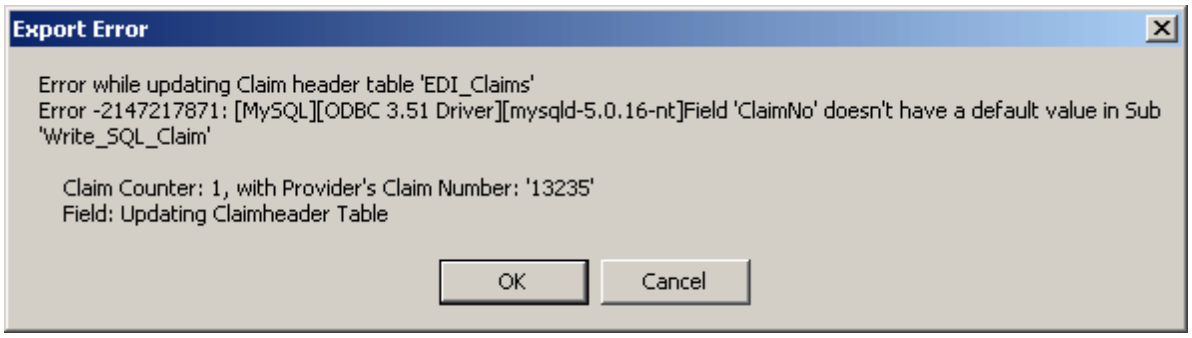
This error happens when a column that was selected for export does not exist in the Header table. In this particular case it is the field 'ClaimNo'. If you receive this error, go back to your table admin tool and check the field 'ClaimNo'

Multi-step OleDB Operation generated errors



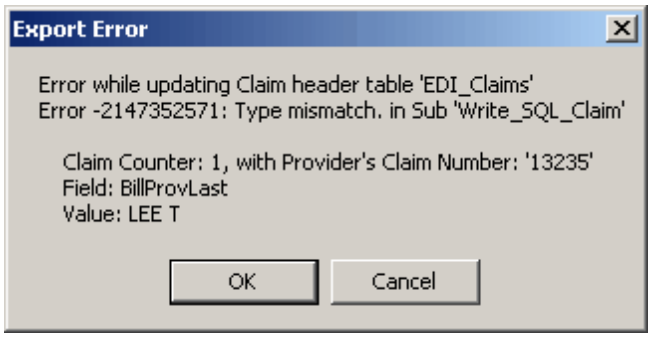
This is typically the message when the field definition in the database is different from the data. Here we see that the error occurred with the billing provider's specialty. The field definition in the table was set as varchar(10) and the value here:000000002331 has 12 digits, causing the error message.

Field doesn't have a default value



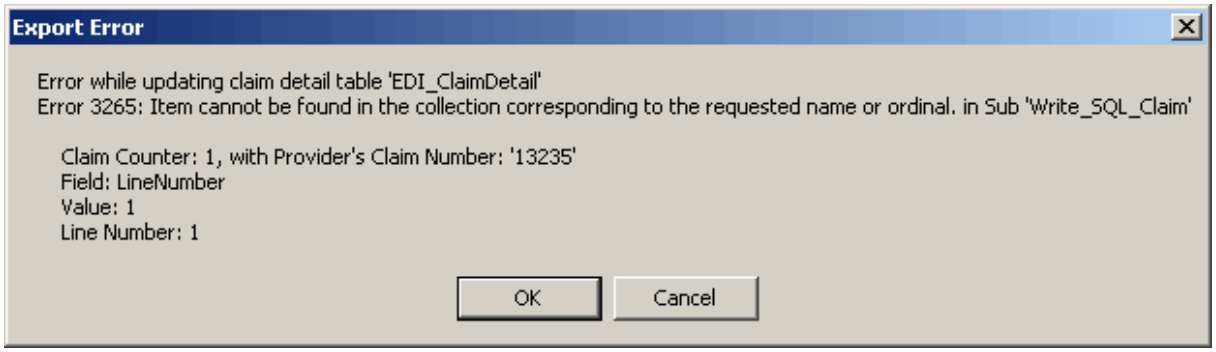
The field 'ClaimNo' is defined as 'Not Null'. But somehow this data was not present and HIPAA Claim Master tried to update the table with a null ClaimNo.

Type mismatch:



This error occurrs when the HIPAA Claim Master tries to write a letter to a field that is defined as 'Integer' for example. The data type of the column does not match the data type of the value.

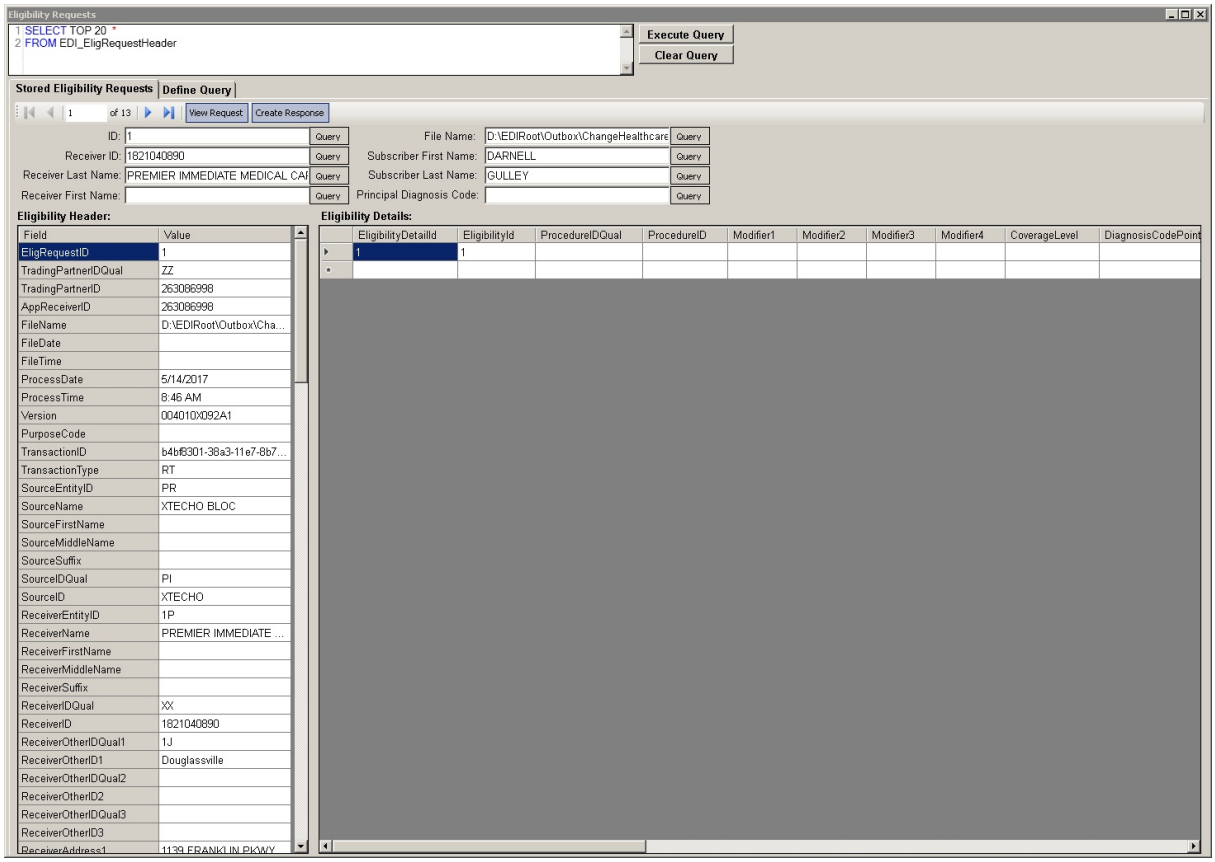
Claim Detail Errors



The errors with the claim detail table are similar, only that the error message indicates also at which line number it occurred.

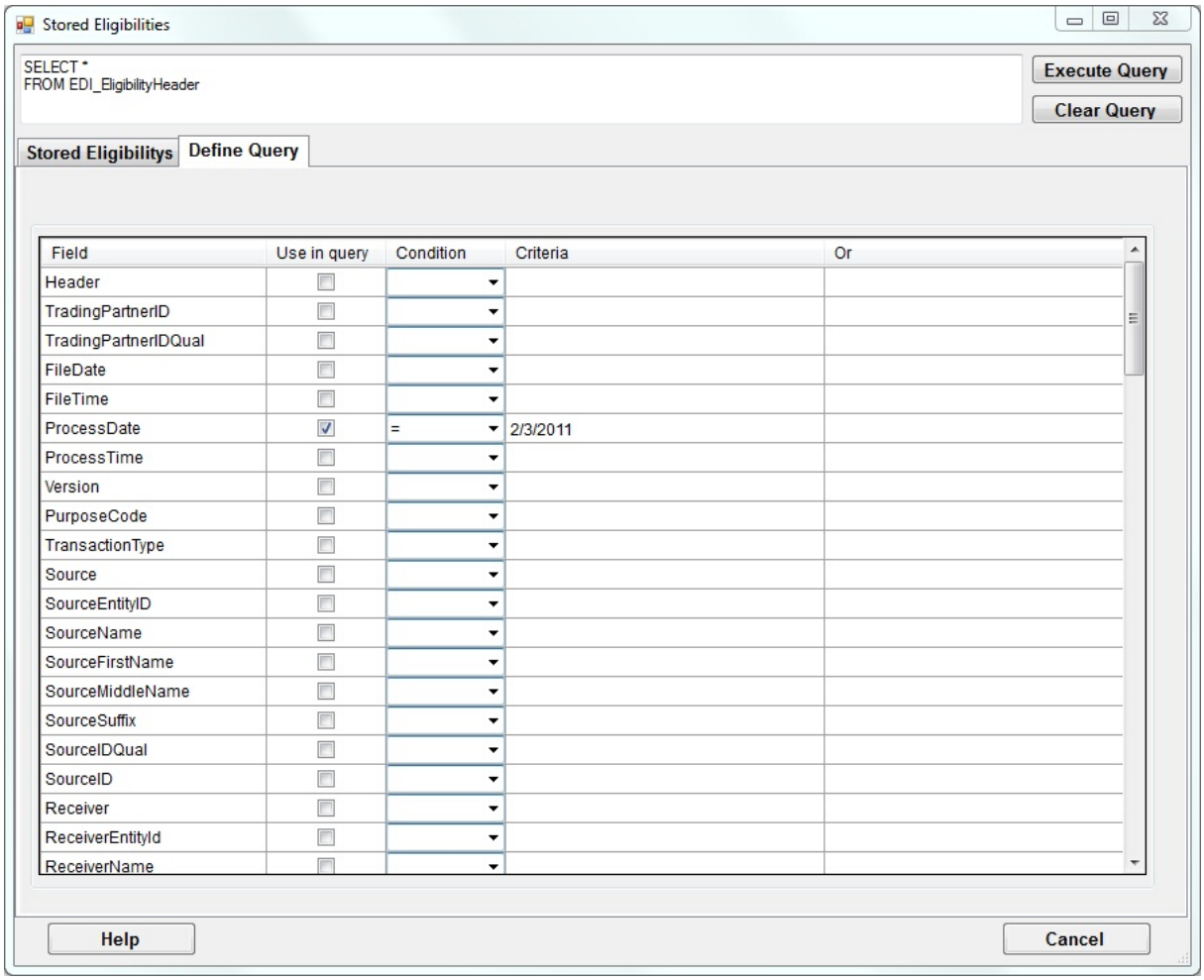
5.8 Exported Requests

You can work with the data in the eligibility tables through the 'Exported Eligibilities" screen.



Stored Eligibility Request records

When you open the screen it shows you the first record in the database and the screen would let you scroll through all the records. You can also enter your own SQL query to select certain records only either as free form query if you are experienced in the database query language or through the 'Define Query' tab

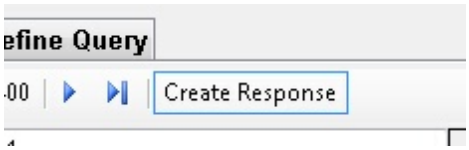


Build your query

Here you can compose your query using the fields in the database and conditions that you select

5.9 Creating Responses from the database

In the 'Stored Eligibility Requests' screen is a button 'Create Response'

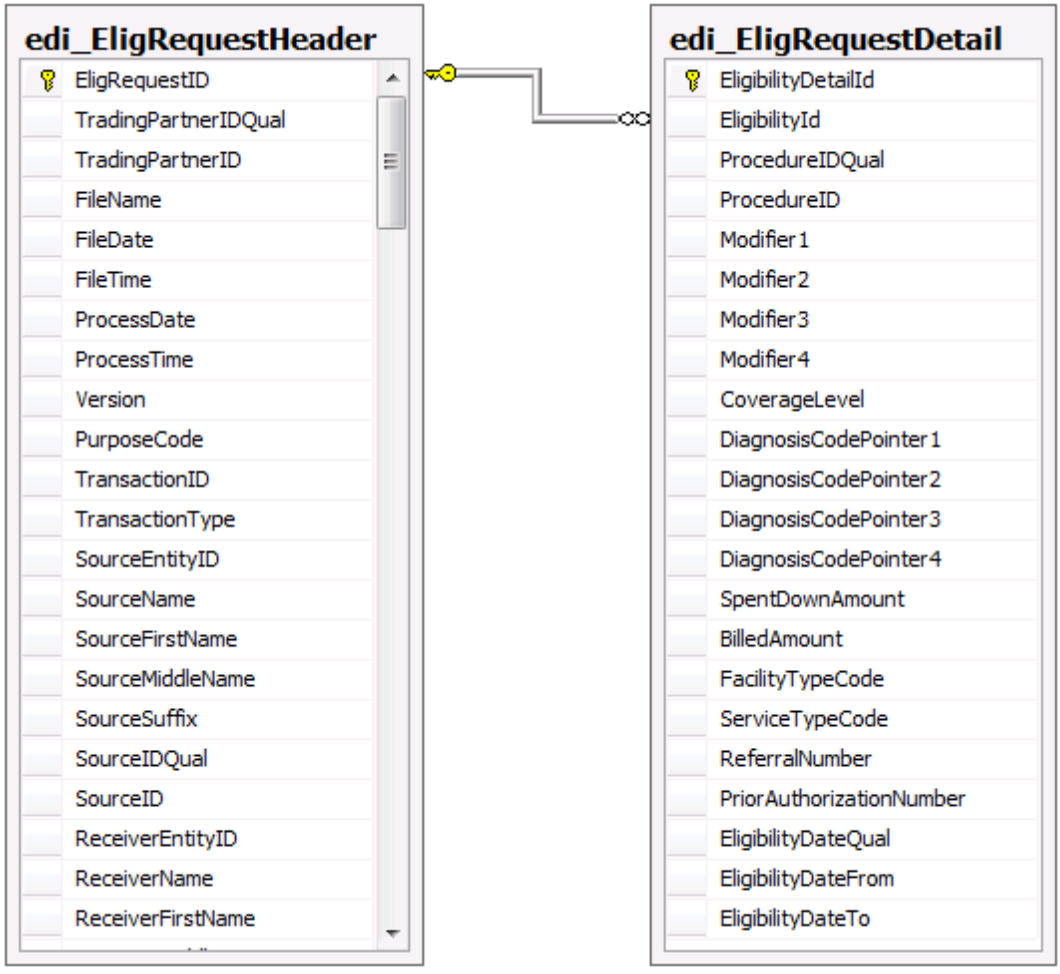


The 'Create Response' button

When you click this button the request is loaded from the database into the create response screen.

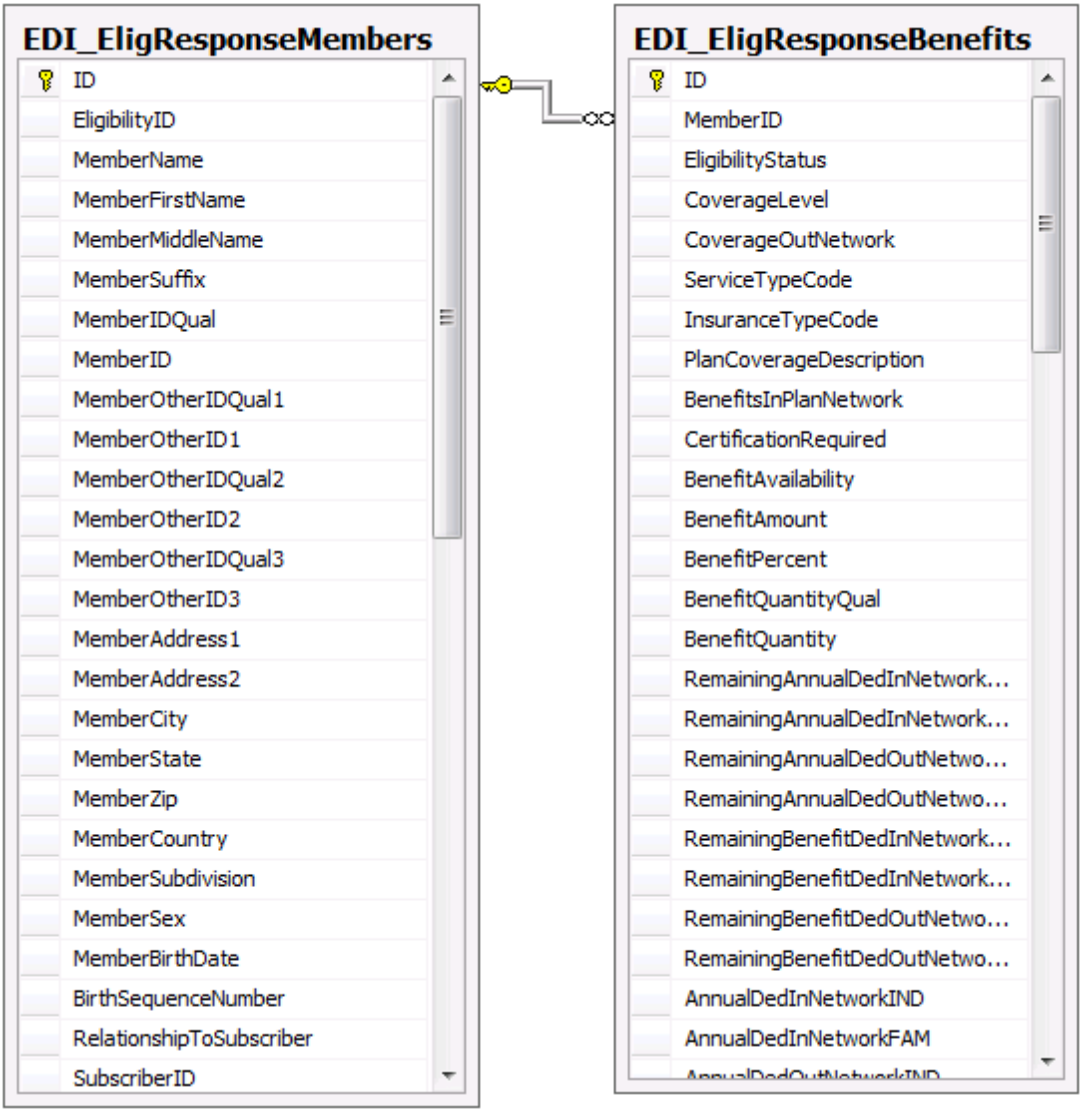
5.10 Database Schema

Incoming 270 request information is stored in two tables named *EDI_EligRequestHeader* and EDI_EligRequestDetail.



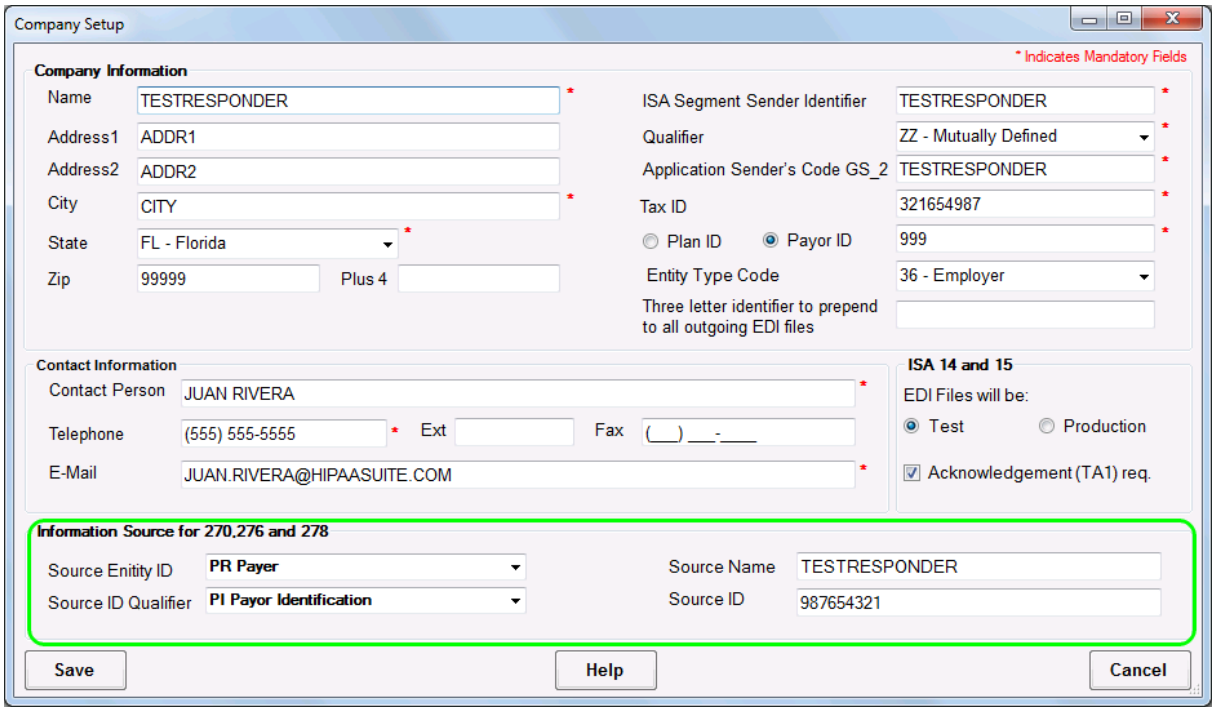
Request Tables schema.

Member/dependent identifying information is stored in *EDI_EligResponseMembers* and any benefit or eligibility information on any given member or dependent is stored in *EDI_EligResponseBenefits*.



Response tables Schema.

In terms of the outgoing EDI file, the table EDI_EligResponseMembers contain information for loop Loop 2000C/2100C and 2000D/2100D respectively, while the table EDI_EligResponseBenefits covers loops 2110C to 2120C and 2110D to 2120D. The loop 2000A, information source detail, is generated dynamically from the Company Setup table. The company setup form has fields reserved for this purpose.

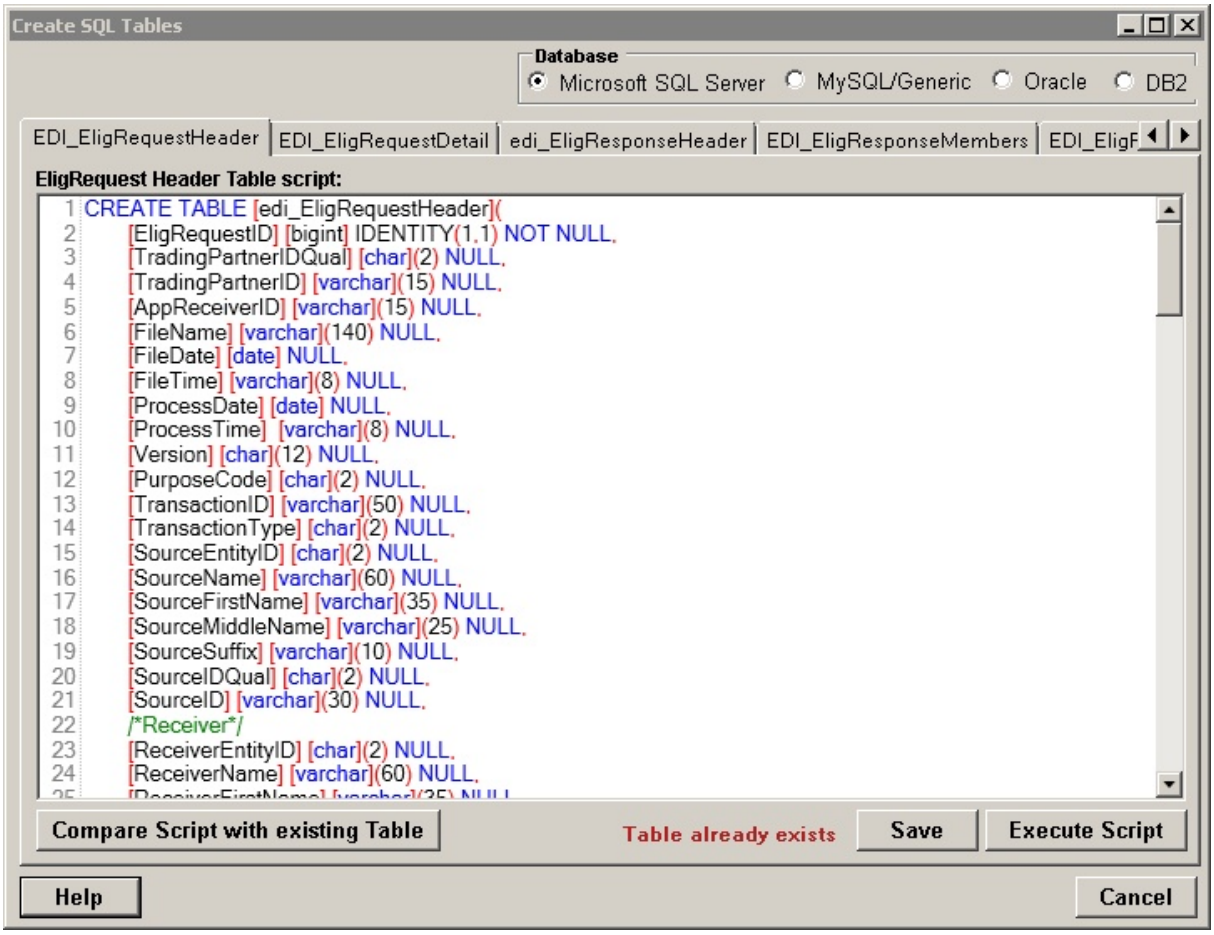


Company Setup screen. Emphasis on Information Source fields.

Loops 2000B/2100B are created from the incoming request's Information Receiver Details.

5.11 Creating Tables

The HIPAA Eligibility Responder can create the tables needed for the export of the data. Once you have the connection to the database configured and tested you can go to the "Create the tables" screen.



SQL scripts to create the eligibility tables, including the response tables

What you see is the SQL scripts to create the tables. The product comes with two versions, one for Microsoft SQL Server, the other for mySQL. If you have a different database you will have to manipulate the scripts until they work. You can change the scripts in this window.

6 Populating Members and Benefits

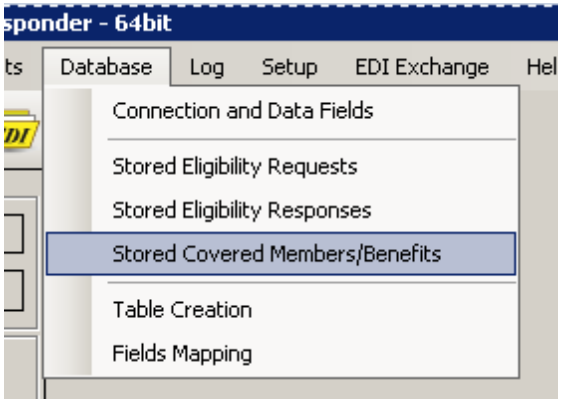
6.1 Concepts

Every row in *EDI_CoveredMembers* represents a single Member or Dependent. Every row in *EDI_CoveredBenefits* stores a single Benefit in its entirety. The Benefit itself is identified by its Service Type Code and MemberID, tying to a specific member; there will be a single row for each Benefit (Service Type Code), of which many can be linked to a

single Member or Dependent. This allows us to fully represent any Member's or Dependent's Eligibility and Benefit information in a database as compactly as possible without losing information.

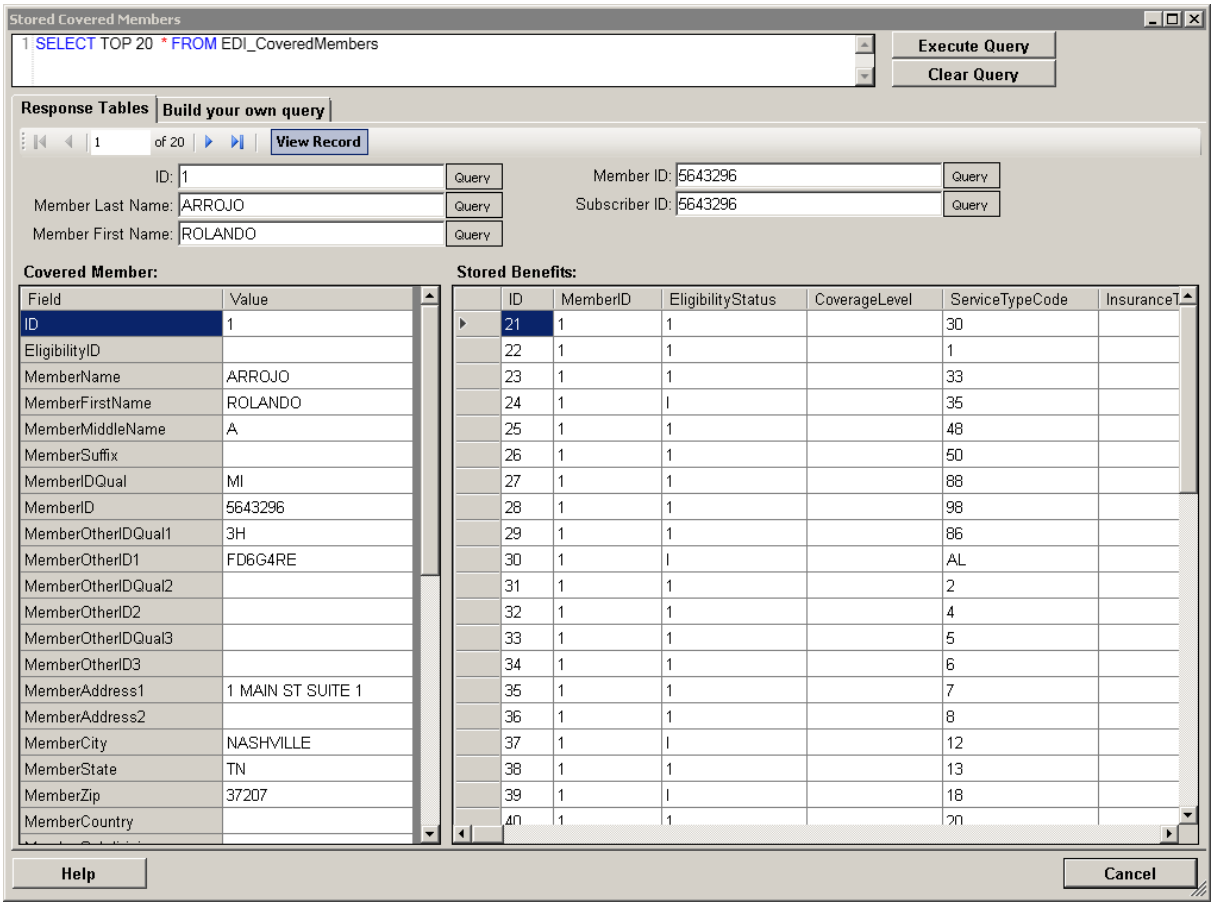
6.2 Members

Member and Dependent information is stored in the EDI_CoveredMembers table and can be viewed easily using the HIPAA Eligibility Responder's Stored Covered Members screen. To open it, select "*Stored Covered Members/Benefits*" from the *Database* menu option.



Stored Members and Benefits menu option.

The window below will appear. From it we can easily search for a member using his or her first and last names and/or member ID.

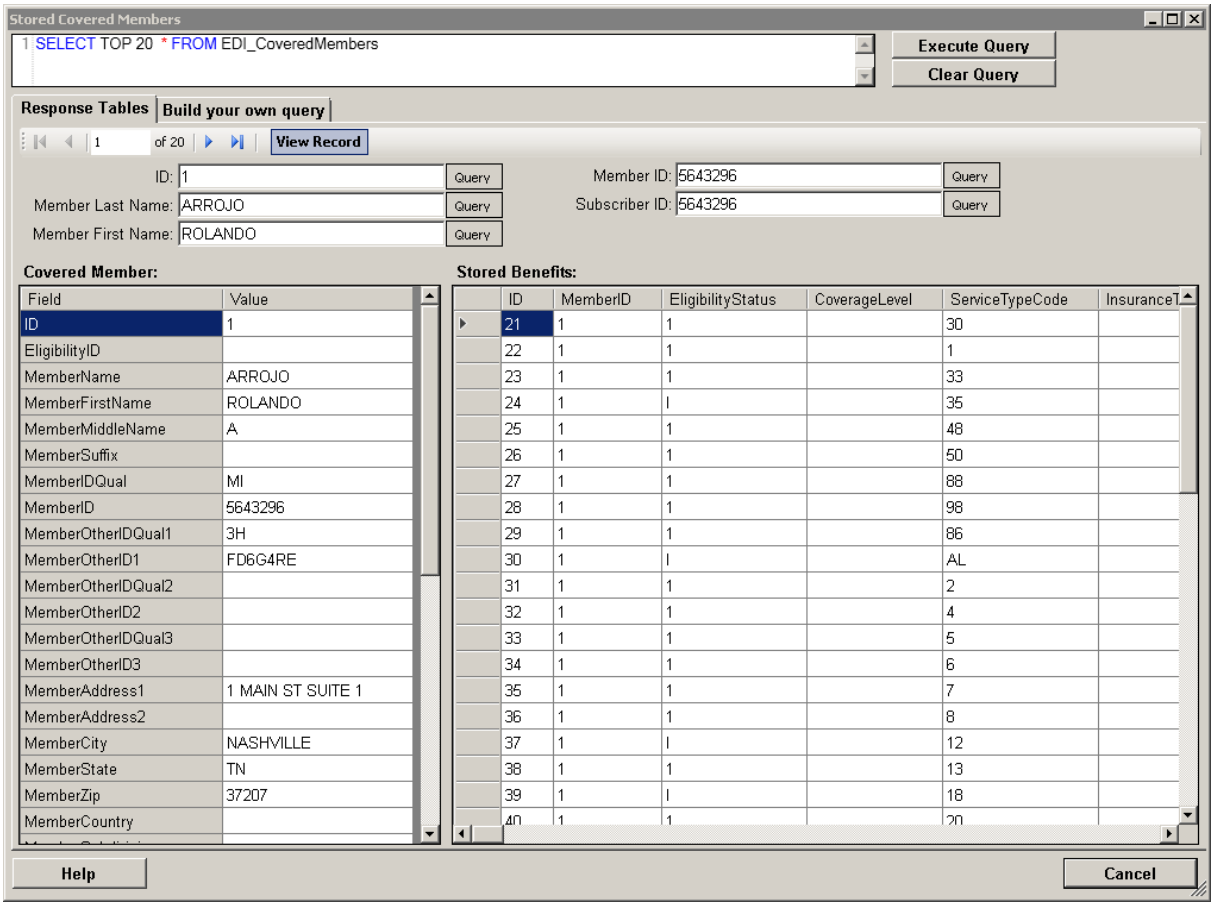


Stored Members and Benefits window loaded with test bed Data example Frank Castillo.

The left side of the presented fields covers all Member information stored in the *EDI_CoveredMembers* table. A Member's full name, address, gender and birth date are stored along with any relevant identifiers such as the Member ID.

6.3 Benefits

The Stored Covered Members and Benefits window also presents all benefits and benefit information specified for a single Member or Dependent. They can be viewed to the right of the Member field and his or her benefits to the left.



Stored Members and Benefits window loaded with TestBed Data Member Frank Castillo.

All eligibility and benefit information is stored in the *EDI_CoveredBenefits* table. Each row represents a single benefit for a single Member, identified by its Service Type Code and MemberID, respectively. The MemberID is an internal field (i.e., this field is not read or written to an EDI file) and corresponds to a single row in the *EDI_CoveredMembers* table.

In the case of a Dependent, who might not have his or her own Member ID, the *Subscriber ID* field is filled with the subscribing Member's MemberID. Otherwise, it is left blank to denote a subscribing Member.

6.4 Monetary Fields

Since every Benefit is represented by a single row in the *EDI_CoveredBenefits* table, we need to make sure all possibilities are accounted for, the alternative being a multitude of rows representing a single ServiceTypeCode and its various combinations of coverage level, deductibles, co-pay and co-insurance amounts. This means all Family or Individual-specific payment amounts and deductibles have to be represented, even those for

different out of network coverage. A number of fields are provided for this and cover Annual Deductible, Remaining Annual Deductible, and Remaining Benefit Specific Deductible for both individual and family coverage both in and out of network. These fields also include co-pay and co-insurance both in and out of network.

Below is an example of a testing data member's eligibility and benefit information grouped by each item's Service Type Code.

Stored Benefits:

ID	MemberID	EligibilityStatus	CoverageLevel	CoverageOutNetwork	ServiceTypeCode
157	4	1			30
158	4	1		Y	1
159	4	1		Y	33
160	4	I			35
161	4	1		Y	48
162	4	1		Y	50
163	4	I			88
164	4	1		Y	98
165	4	1		Y	86
166	4	I			AL
167	4	1		Y	2
168	4	1		Y	4
169	4	1		Y	5
170	4	1		Y	6
171	4	1		Y	7
172	4	1		Y	8
173	4	1		Y	12
174	4	1		Y	13

TestBed Data Member example Frank Castillo's Benefits.

Below is an excerpt highlighting the multiple benefit coverage option fields as would be filled in a typical covered member's set of eligibility rows depicting the Status of each benefit, its Service Type Code, and deductible information.

EligibilityStatus	ServiceTypeCode	PlanCoverageDescription	RemainingAnnualDedInNetworkIND	RemainingAnnualDedInNetworkFAM	AnnualDedInNetworkIND	AnnualDedInNetworkFAM
1	30	Tennessee PCN	50.00	300.00	250.00	500.00
1	1	NULL	NULL	NULL	NULL	NULL
1	33	NULL	NULL	NULL	15.00	20.00
I	35	NULL	NULL	NULL	NULL	NULL
1	48	NULL	NULL	NULL	NULL	NULL
1	50	NULL	NULL	NULL	NULL	NULL
1	88	NULL	25.00	50.00	25.00	75.00
1	98	NULL	NULL	NULL	NULL	NULL
1	86	NULL	NULL	NULL	NULL	NULL
I	AL	NULL	NULL	NULL	NULL	NULL
1	2	NULL	NULL	NULL	NULL	NULL
1	4	NULL	0.00	0.00	0.00	0.00
1	5	NULL	0.00	0.00	0.00	0.00
1	6	NULL	NULL	NULL	NULL	NULL
1	7	NULL	NULL	NULL	NULL	NULL

Deductibles for plan and benefits.

7 Automating File Processing

7.1 Using Command Line Arguments

The HIPAA Eligibility Responder can accept command line arguments. The following is the list of the command line arguments; they must be separated by commas.

1. The first command line argument is the **filename** or the **directory path**.

2. The second argument contains the processing options. The following argument may be used:

X - Export to database.

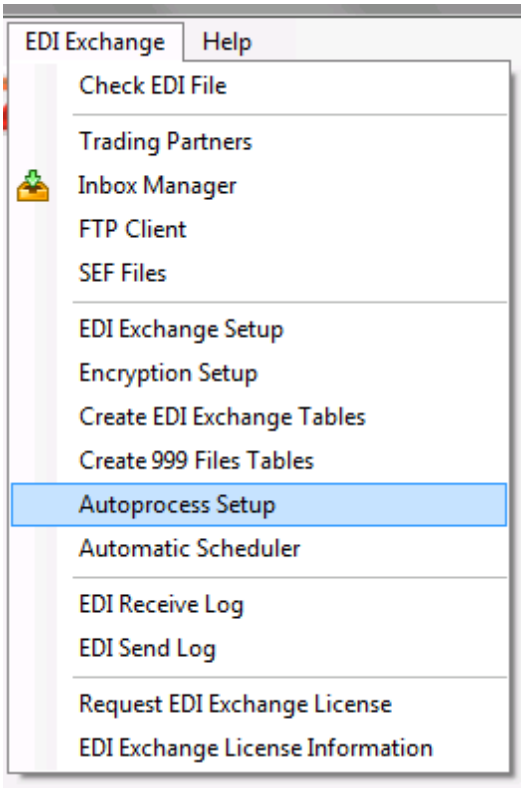
Example: To export an Eligibility Request to the database:

```
C:\Program Files\HIPAAsuite\HIPAA Eligibility Responder>HIPAAEligibilityResponde
r.exe D:\EDI\270_1.edi,X
```

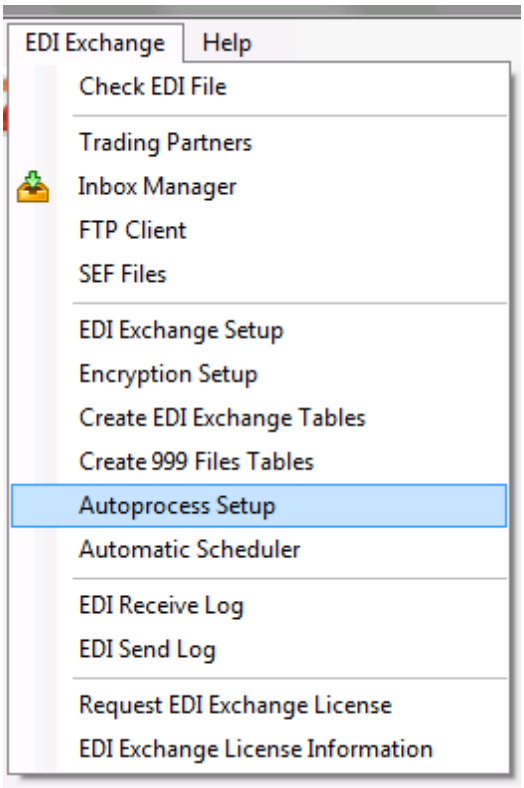
7.2 Autoprocessing with the EDI Exchange Module

Autoprocessing the Inbox

When processing from the command line with the EDI Exchange module enabled, the argument you need is "Auto". The directory used to look for new files and the processing options are defined in the setup screens for EDI Exchange. No further arguments are needed.

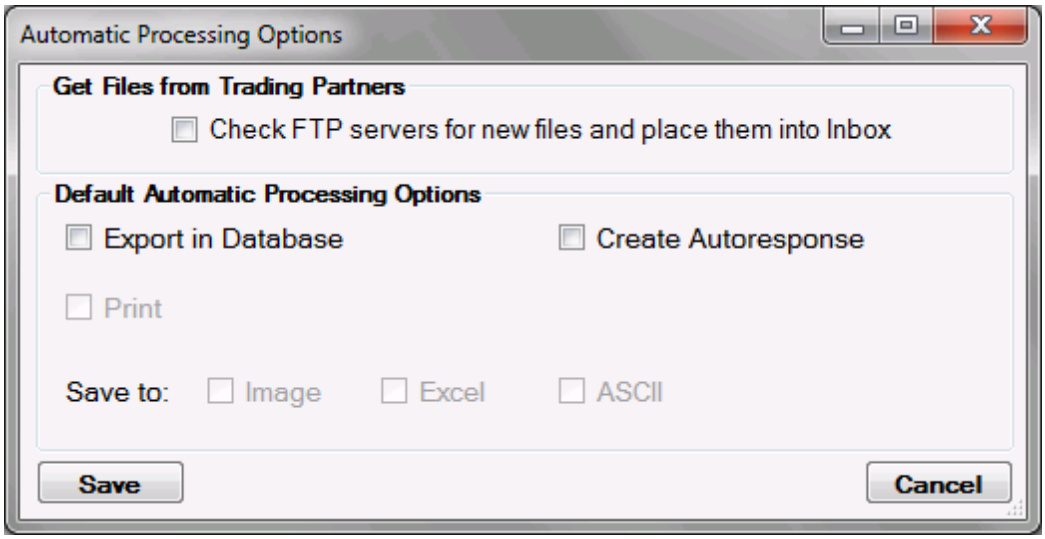


To setup autoprocess options, go to EDI Exchange ▸ Autoprocess Setup:



Autoprocess Setup option in EDI Exchange menu

Any options selected for autoprocessing will carry over to the command line.



EDI Exchange Automatic Processing options

Autoprocessing a Single File

To run a single file through the autoprocessor, add the full filename as second argument to your command.

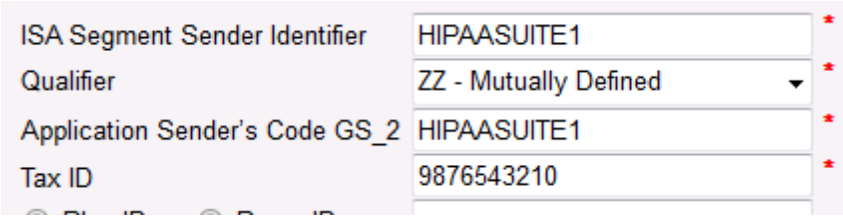
```
C:\Program Files\HIPAAsuite\HIPAA Eligibility Responder>HIPAAEligibilityResponde
r.exe auto,D:\EDI\270_1.edi
```

Command to autoprocess a single file.

7.3 Changing the Default Company

The default company is the identity you assume as the sender when creating EDI files. This affects the ISA, GS, and NM1 sender segments. A single entity may have a need to act as multiple sender identities and so has a need to change the information in the EDI envelopes.

The default company can be changed using command line arguments, affecting the ISA and GS sender ID segments.

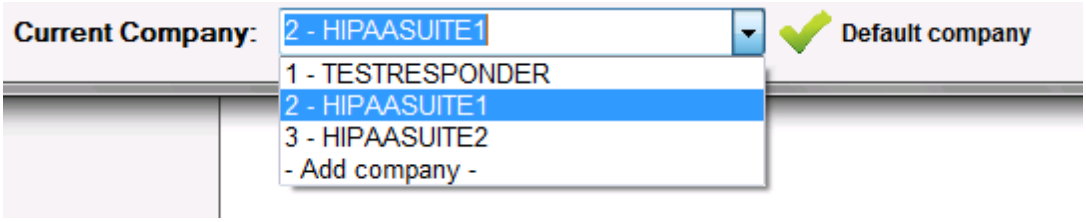


Sender ID segments in Company Setup

To change the default company, a single argument is needed. "**Setcompany**" followed by the company ID of the company you wish to set.

```
"setcompany <ID>"
```

The Company's ID in this case is not its EDI identifier, but the value of the ID row in the COMPANY_SETUP table. It can also be found in the Company Setup window:



Company selection in Company Setup

Example

The command argument **`setcompany 3`**

```
C:\Program Files\HIPAAsuite\HIPAA Eligibility Responder>HIPAAEligibilityResponde
r.exe setcompany 3
```

will set the default company to ID = 3, which is HIPAASUITE2 in the example picture above. The log entry for this command will be

```
Set default company with ID 3
        Company # 3 is set as a default company
```

Excerpt from log. Default company changed.

8 Automatic Responses

8.1 Introduction

As mentioned earlier, The HIPAA Eligibility Responder can autoprocess Eligibility Requests and Functional Acknowledgments without the need to launch the program's User Interface. To do this, the HIPAA Eligibility Responder can accept command line arguments. The following is a list of the command line arguments; they must be separated by commas.

1. First Argument - mode

   a. "auto" will process a 270 file. If no other arguments are included, all 270 files in the EDI Exchange Inbox directory will be processed. Any other files in the Inbox directory will be ignored. If the filepath is included as a second argument, that file will be processed individually.

   b. "soap" will process a specific 270 or 999 file. A second and third argument containing the file directory (including filename) and PayloadID are necessary.

   c. If a filepath is used instead, only one more argument is necessary.

2. Second Argument – full filepath (auto, optional / soap)

   a. Not necessary for "auto" process mode. If included will only autoprocess that file.

   b. Necessary for "soap" mode.

   c. If a filepath was used as a first argument, the following processing options may be used:
      X - Import file to database.

3. Third Argument – PayloadID (soap only)

   a. SOAP/MIME PayloadID tied to request/response transaction. Necessary to identify request, response, and acknowledgements associated with a single transaction.

4. Fourth Argument – FileType (soap only, optional)

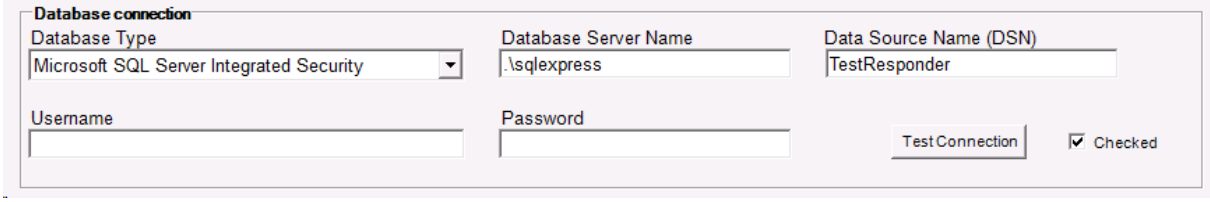
   a. Used to differentiate between a request file and an acknowledgment file. If omitted, file will be processed as a 270 request.

The HIPAA RealTime Server can also be used to run the Eligibility Responder without the need for user interaction. It can accept 270 EDI Eligibility Request transactions, draw eligibility data stored in the Eligibility tables, and send a 271 Eligibility Response in under 10 seconds.

8.2 RealTime Server

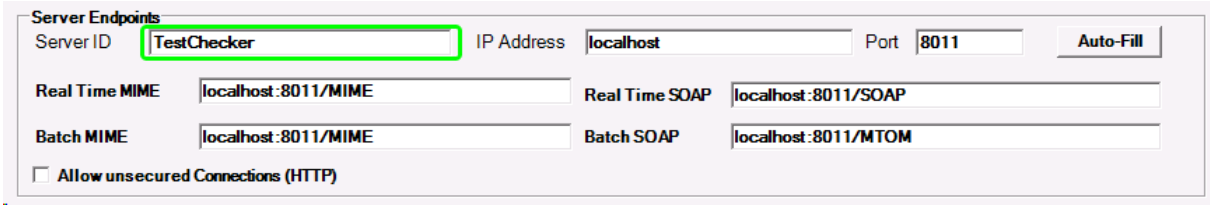
The HIPAA RealTime Server can be used in conjunction with any HIPAAsuite Responder application to provide MIME/SOAP functionality as described in CAQH CORE Phase II. This means the HIPAAsuite Eligibility Responder will be CAQH CORE compliant, being able to answer 270 Real-Time and Batch mode messages in both SOAP and MIME formats.

To respond to SOAP or MIME 270 Eligibility requests, the HIPAA RealTime Server must be configured to use the same database as the HIPAA Eligibility Responder. This serves to provide the RealTime Server with information such as the Trading Partner's ID and credentials. If the incoming SOAP/MIME request's SenderID is not the Trading Partner ID associated with a username/password, the message will be rejected. The following is a part of the RealTime Server's configuration window:



The Database used by the RealTime Server must be the same used by the Eligibility Responder.

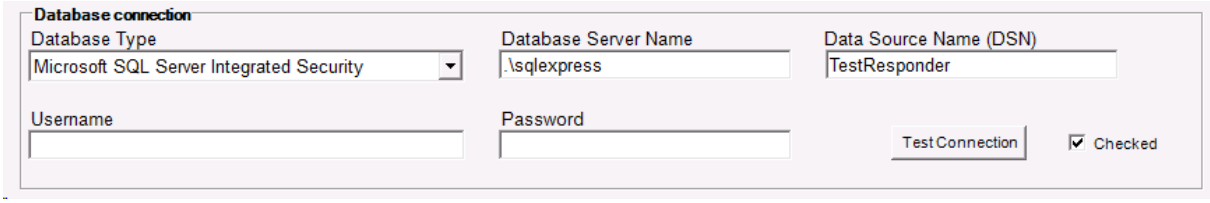
The name specified in the HIPAA RealTime Server's Server ID field is the name that will be used to identify you or your organization in the SOAP and MIME Sender/Receiver ID fields.



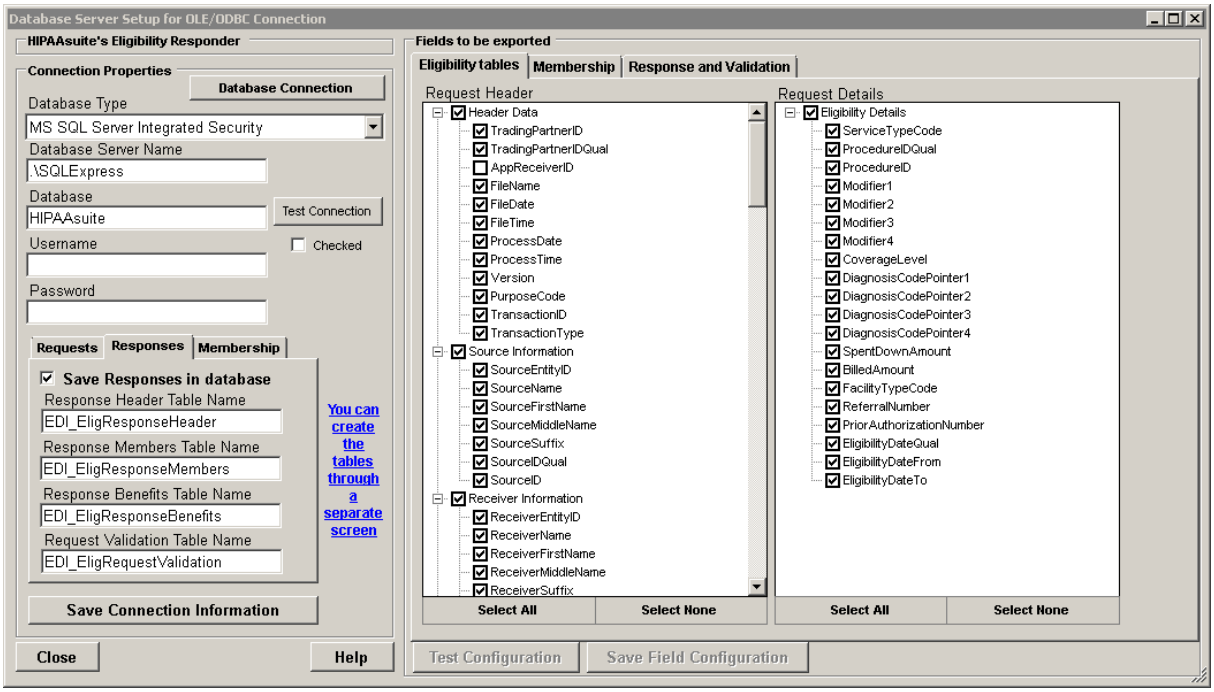
This will be your ID when sending/receiving SOAP or MIME messages.

8.3 Server Setup

In order for the HIPAA RealTime Server to know what to do with a particular incoming 270 request, an outgoing 271 response, or a 999 acknowledgment, it is necessary to use the same database as the HIPAA Eligibility Responder.

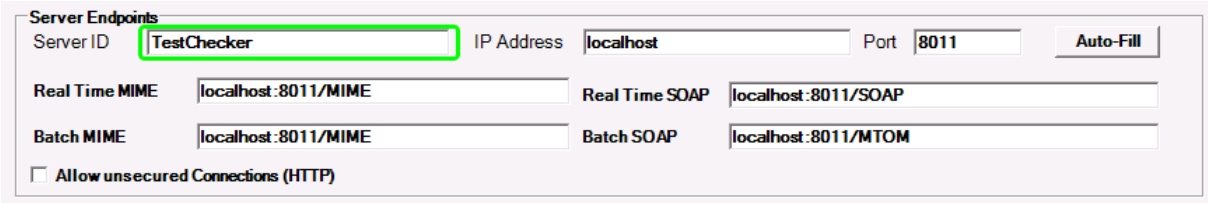


RealTime Server Database configuration.



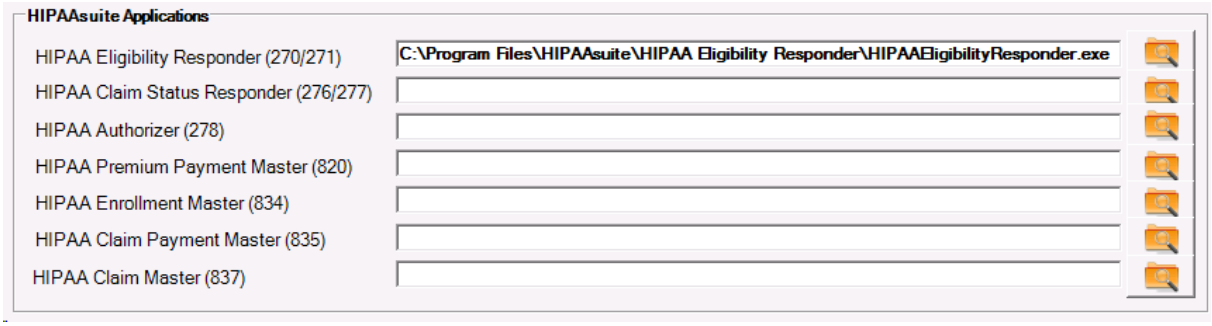
Eligibility Responder Database Configuration.

The server should also be using the desired Trading Partner ID to identify you or your organization as the recipient when processing incoming messages and as a sender when responding to messages.



Part of RealTime Server configuration. Emphasis on ServerID.

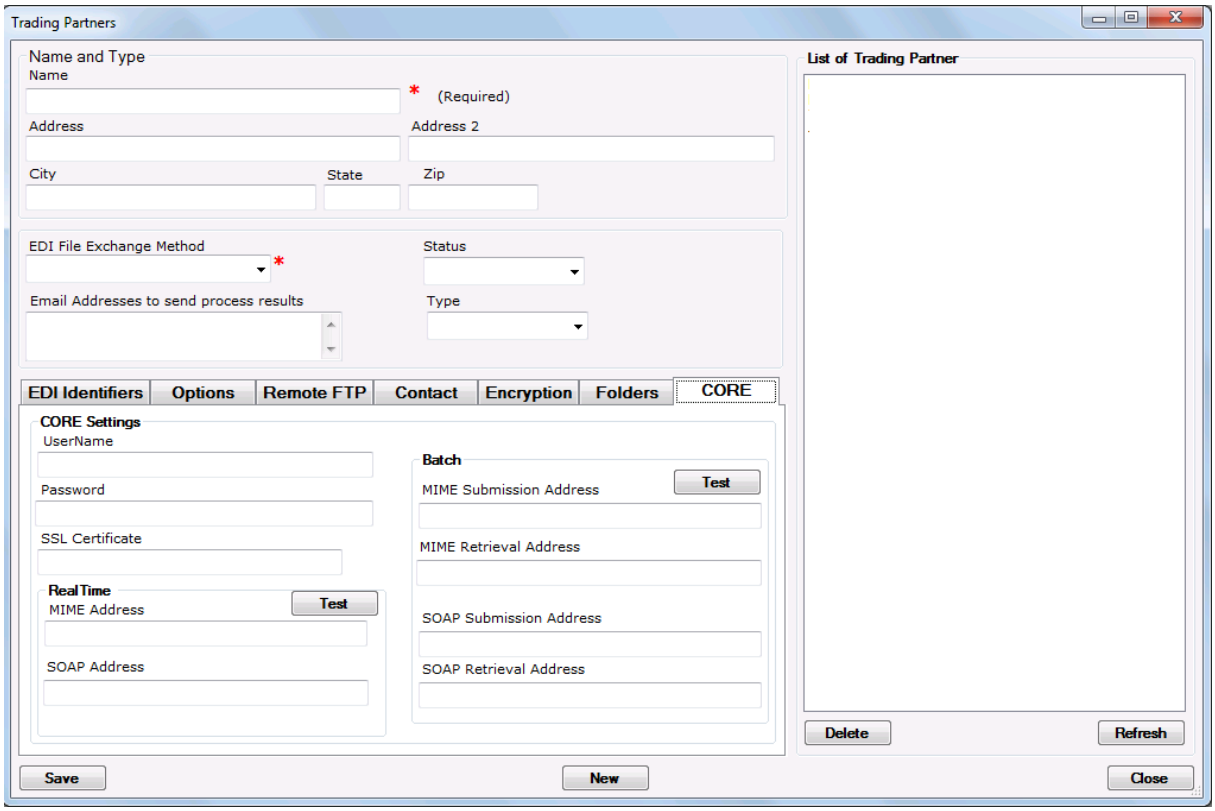
Finally, the full HIPAA Eligibility Responder path must be included in the *HIPAAsuite Applications* section of the RealTime Server setup screen. If the default install location was used, the HIPAA Eligibility Responder's path will be *C:\Program Files (x86)\HIPAASuite\HIPAA Eligibility Responder\HIPAAEligibilityResponder.exe* if the x64 bit version was installed. For the x32 bit version *C:\Program Files\HIPAAsuite\HIPAA Eligibility Responder\HIPAAEligibilityResponder.exe* will be the default directory.



The Eligibility Responder's directory.

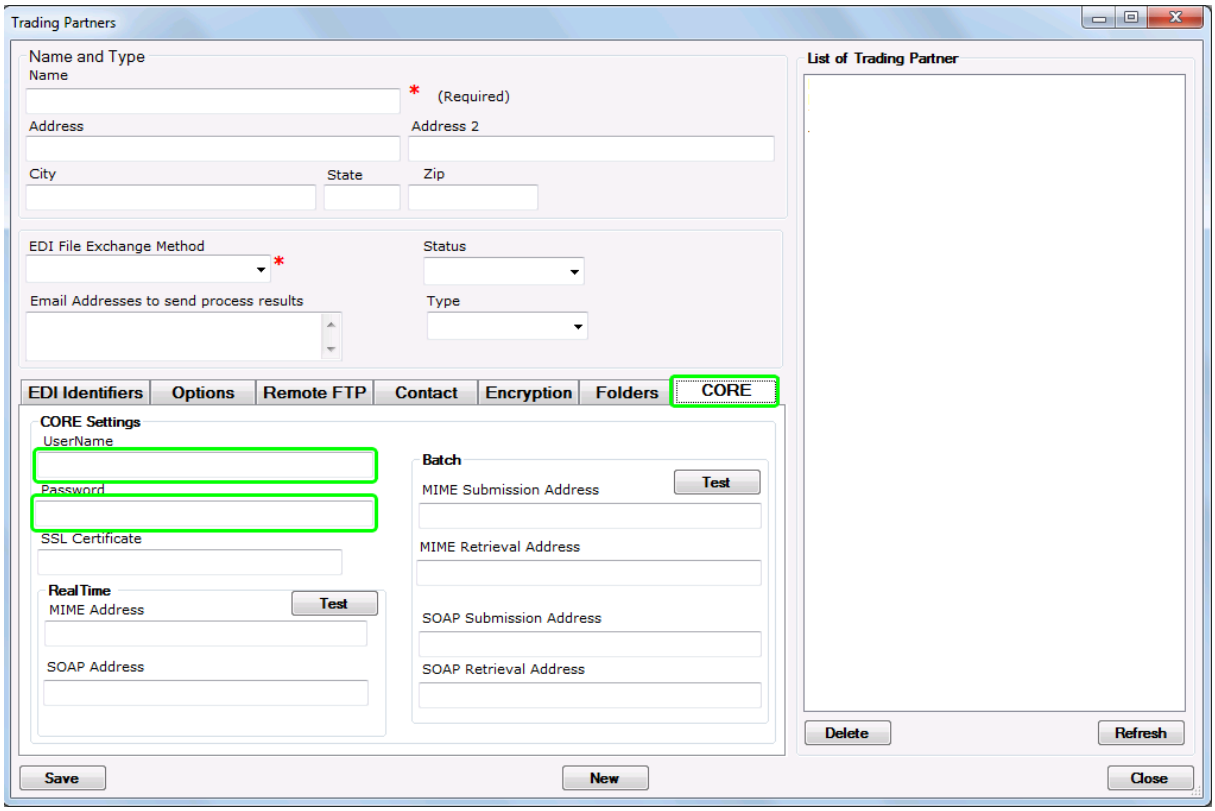
Trading Partners

To set up a Trading Partner to use your HIPAA RealTime Server, both the HIPAA Eligibility Responder and HIPAA RealTime Server must be using the same database. In the Eligibility Responder's Trading Partner setup screen, select the desired Trading Partner or make a new one.



New Trading Partner.

Having a Trading Partner selected, the CORE tab can be populated with the correct values. Necessary fields to respond to a Trading Partner are a Username and Password. These are set in the Eligibility Responder and read by the RealTime Server and serve as the Trading Partner's MIME/SOAP username key authentication credentials.



Username/Password fields are used by the RealTime Server to authenticate Trading Partners.

This is all the setup necessary on our end. Inform the Trading Partner of their username key credentials and your RealTime Server's addressing and your Trading Partner will be able to request and receive Eligibility information from your server.

9 EDI Exchange

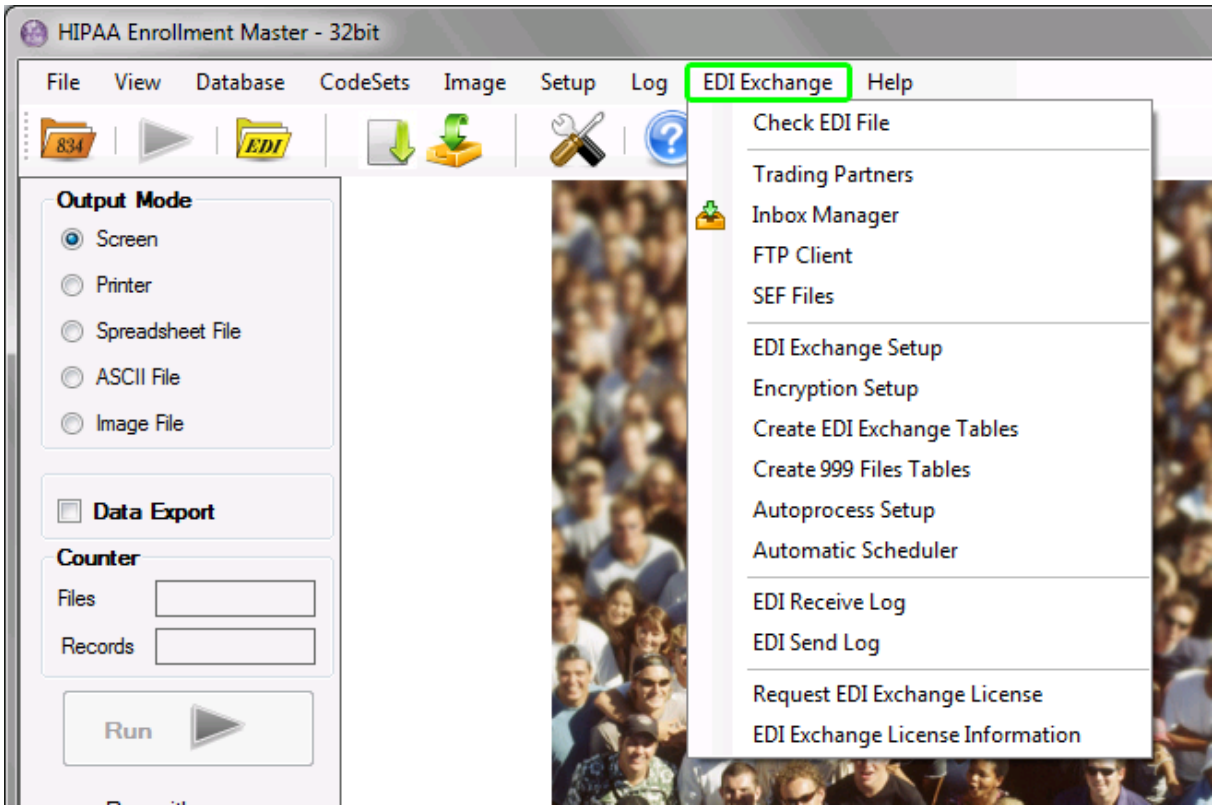
9.1 Getting Started

9.1.1 About EDI Exchange

EDI Exchange is a module available in most HIPAAsuite EDI applications. It is an option that you can purchase for an additional cost. Some of our products, such as HIPAA Claim Master, process EDI files but do not receive or send EDI files to and from your trading partners. EDI Exchange is created to do that. EDI Exchange is designed for those organizations that have a large volume of EDI files, need more order and automation and adhere to tougher compliance rules. The EDI Exchange is an EDI pre-processor that handles FTP transport, encryption, HIPAA compliance check, trading partner management, etc. Outgoing EDI files can be checked for compliance; individual records

that do not pass the check can be withheld.

HIPAAsuite products with EDI Exchange module have a main menu item called "EDI Exchange" with sub-menus to call the module's functions.



The "EDI Exchange" menu in HIPAA Enrollment Master

EDI Exchange performs the following functions:

- **Trading Partners Management** — The following Trading Partner's parameters can be stored and transparently managed with the help of EDI Exchange: name, address, EDI identifiers, delivery methods, encryption parameters, FTP servers, CORE-Compliant server addresses and credentials, communication numbers and folders to keep files separated, special requirements specific to this trading partner. Read more in Setting up Trading Partners.
- **File Transport** — EDI Exchange has a built-in FTP client that can securely connect to your trading partner's FTP servers. If you employ your own FTP server, you can utilize the folder structure that EDI Exchange uses to manage incoming files, users, home directories and permissions so that your Trading Partners can drop off and pick up EDI files. Supported are:
  - **Simple FTP**

  - **FTP Secure**
    - **Implicit FTPS**
    - **Explicit FTPS**
  - **Secure Shell FTP or sFTP**

  Read more in Using FTP Client.

- **Encryption** — Many healthcare-related companies use encryption to cloak the content of their EDI files. The prevalent method of encryption is **PKI** (Private Key Infrastructure) that uses the product of two incredibly large prime numbers as cipher. EDI Exchange supports **PGP** (Pretty Good Privacy), the leader in PKI products as well as the open source **GPG** project with its Windows sub project PGP4Win. Both are implementations of the same encryption mechanism. Read more in Using Encryption.
- **File Management** — EDI Exchange uses a clear directory structure to store EDI files. The structure is based on root directories for incoming files, outgoing files, processed files and suspended files. Below these root directories, there are subdirectories for each trading partner and then each transaction set. Read more in Defining Root Directory and Initializing EDI Exchange.
- **EDI Compliance Check** — EDI standards are strict and precise; adherence to the standards is very important so that any organization can work with them regardless of their backend system software. EDI Exchange has a built-in compliance engine that checks incoming files for compliance. The engine also generates a report listing each problem with the exact location. Outgoing EDI files can also be checked and you have an option to withhold individual records that violate the rules. Read more in Checking EDI Files.
- **EDI Control for Transactions** — The EDI protocols have a few supporting transaction sets that are useful to the smooth functioning of EDI exchanges. They provide the sender with an instant feedback on receipt. The following transaction sets are available:
  - **TA1 Acknowledgment**
  - **997/999 Functional Acknowledgment**
  - **277U/277CA Unsolicited Claim Status Response** (in case of Claims)
- **Logging** — EDI Exchange has several logs that are instrumental to keep processing in order and allows to forensically investigate mishaps. There are three logs in EDI Exchange:

- **Incoming file log** – See Accessing EDI Receive Log.
- **Outgoing file log** – See Accessing EDI Send Log.
- **Daily transaction log**

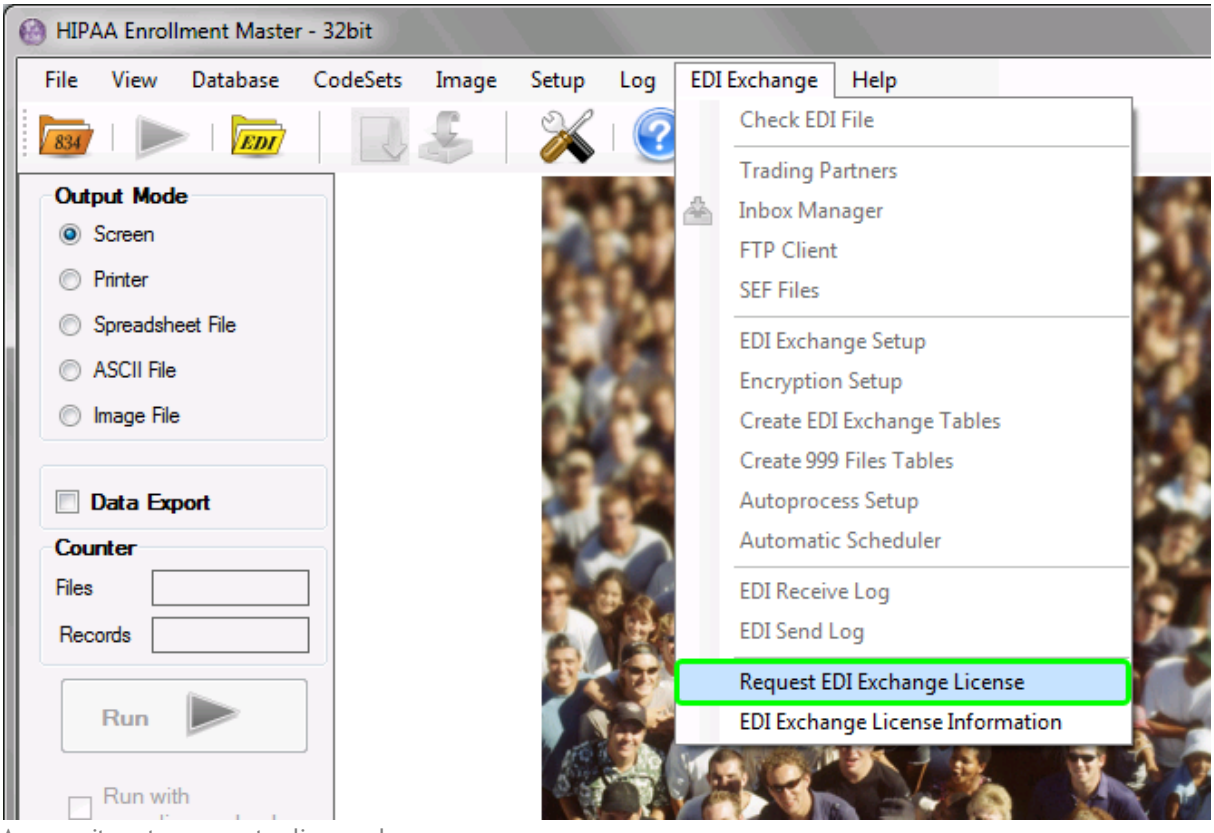
9.1.2 Requesting EDI Exchange License

If your trial has expired, you can request an extension to the trial.

If you purchased the product and need a final license key, you should request an EDI Exchange license.

Follow the instructions below to request a trial or final license key.

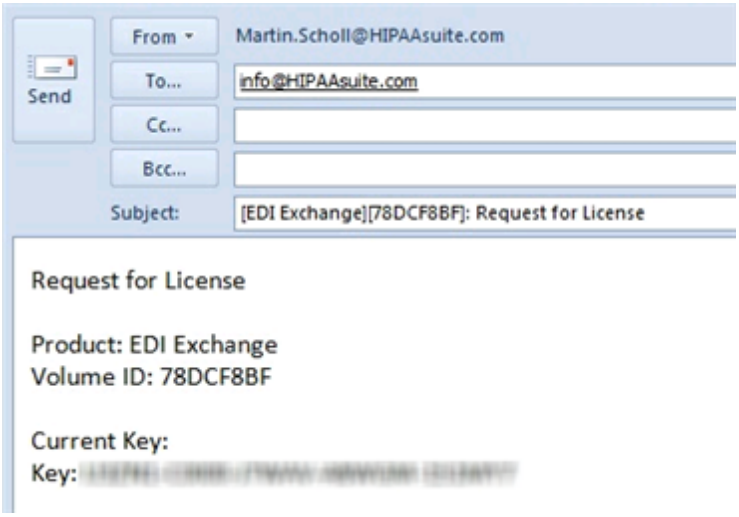
1. Select "Request EDI Exchange license" under the "EDI Exchange" menu item.



A menu item to request a license key

2. Once you have clicked this menu item, your default email application appears. In our case, it is Microsoft Outlook. All information necessary to produce the key is

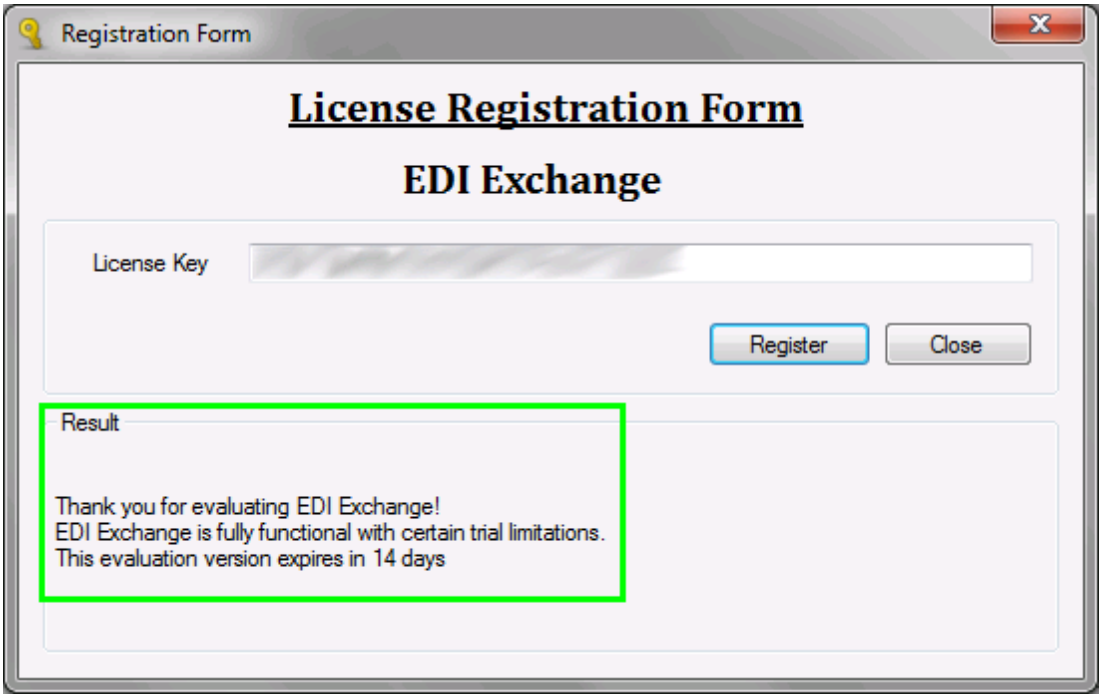
automatically filled out.



Email message created by EDI Exchange

3. You can add a trial extension or a final key after purchasing or relocating the software.

   Once you receive the response with the key for EDI Exchange, you can bring the "Registration Form" screen up again and click on "Register". Enter the key to unlock EDI Exchange. In the Result area, you will see that EDI Exchange has been registered.

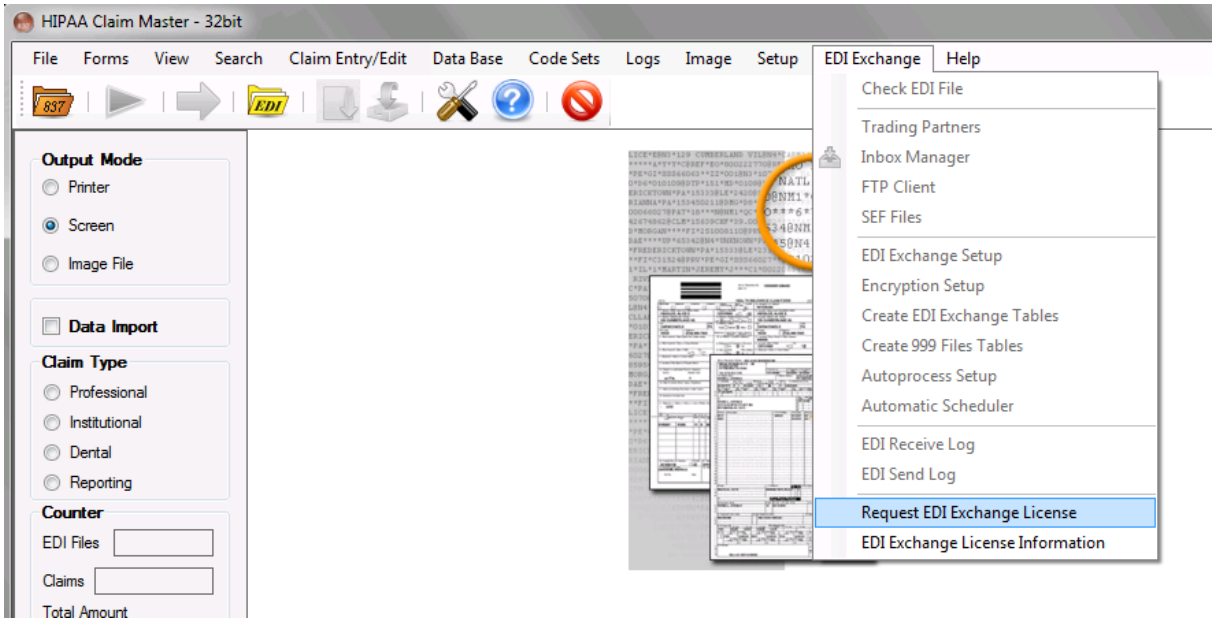


Entering the license key

9.1.3 Registering EDI Exchange

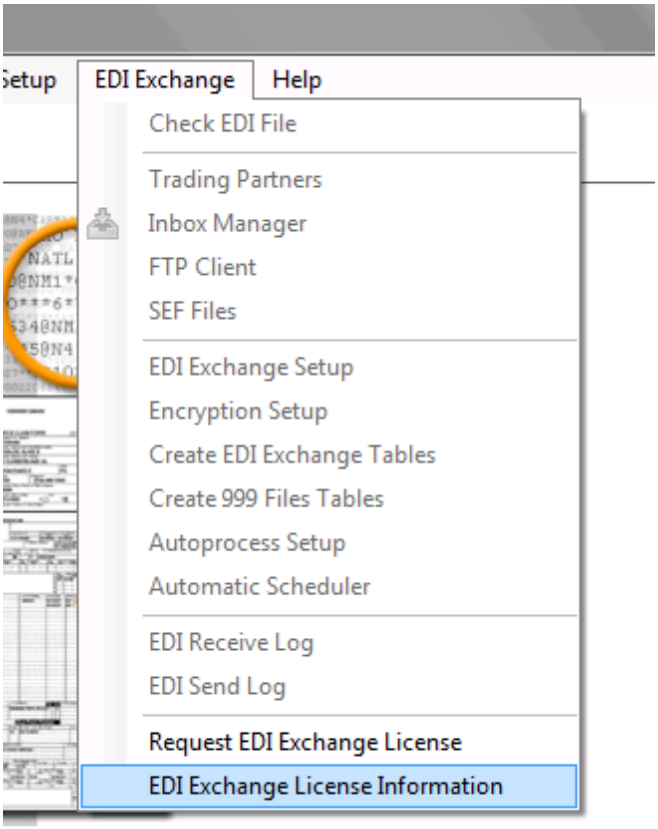
EDI Exchange is licensed separately from the host application, HIPAA Claim Master, for example. The reason is that EDI Exchange will work on all HIPAAsuite Products that are installed on your particular computer. For example, if you have HIPAA Claim Master and HIPAA Enrollment Master licensed, only one license of EDI Exchange is needed and the module will work across two products.

When you first install a HIPAAsuite product of your choice, a 15-day EDI Exchange trial is included. Once the trial expires, EDI Exchange loses its functionality. The menu items under "EDI Exchange" become disabled except the last ones that allow you to license and enable the product.



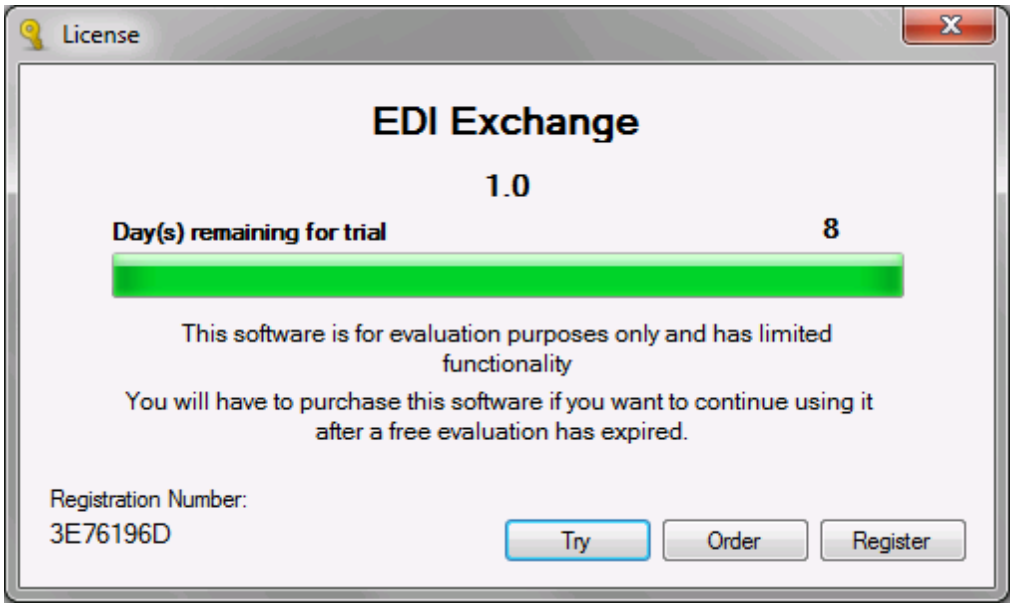
The "EDI Exchange" menu with menu items disabled

You can register the product by clicking on the "EDI Exchange License Information" option under the "EDI Exchange" menu.



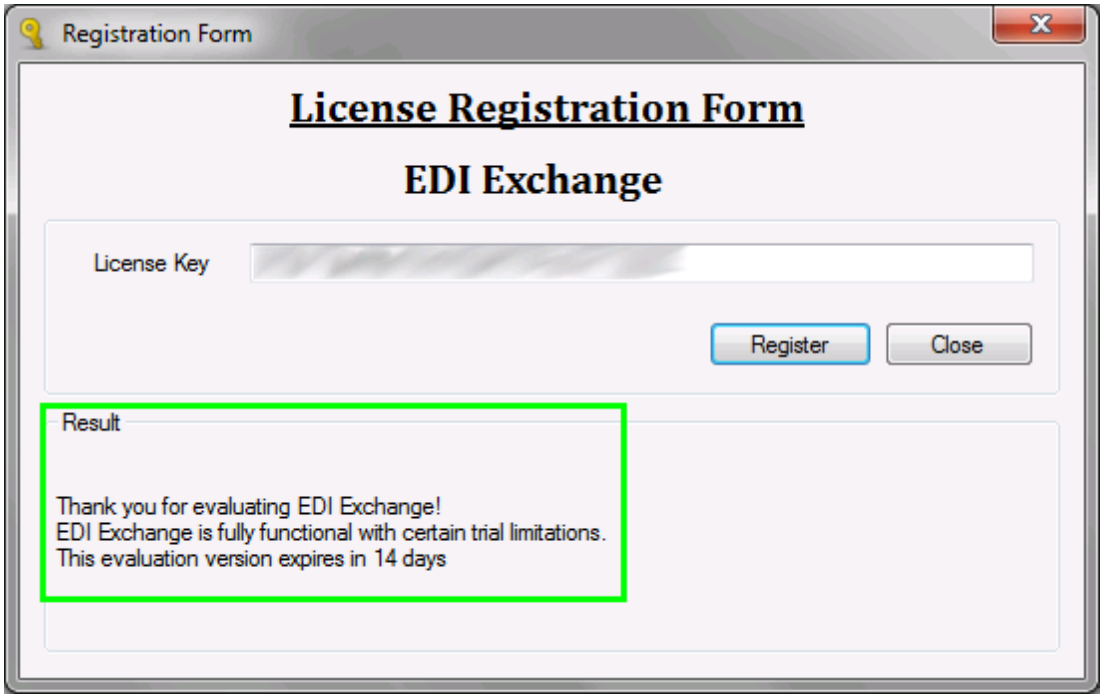
"EDI Exchange License Information" option under the "EDI Exchange"

Then the license screen appears. In the lower left corner you can find the unique registration number needed to create either trial extensions or final licensing.



The license information screen

Once you click on "Register," you can enter the license key that you have previously received via email from us (see Requesting EDI Exchange License.) Click on "Register" and you will see the registration message in the "Result" area.



Extending the trial by entering a license key

Close the "Registration Form" and continue using the EDI Exchange.

9.2 Configuring EDI Exchange (Obligatory Settings)

9.2.1 1 Setting up Database Connection

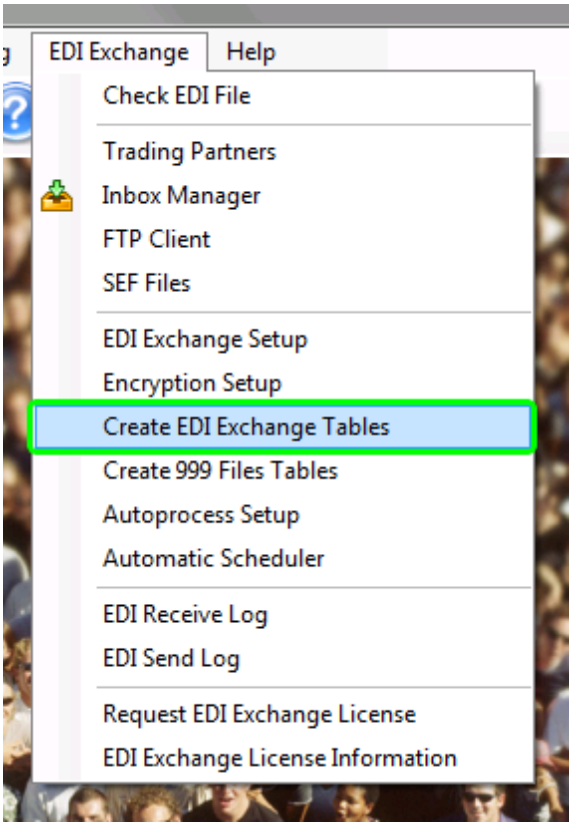
EDI Exchange work is based on the database connection that you define under *Database ▸ Connection and Data Fields* in the main menu of the HIPAA host application. Make sure the connection has already been set up and tested before proceeding with EDI Exchange.

Then proceed to the next step: Creating Database Tables.

9.2.2 2 Creating Database Tables

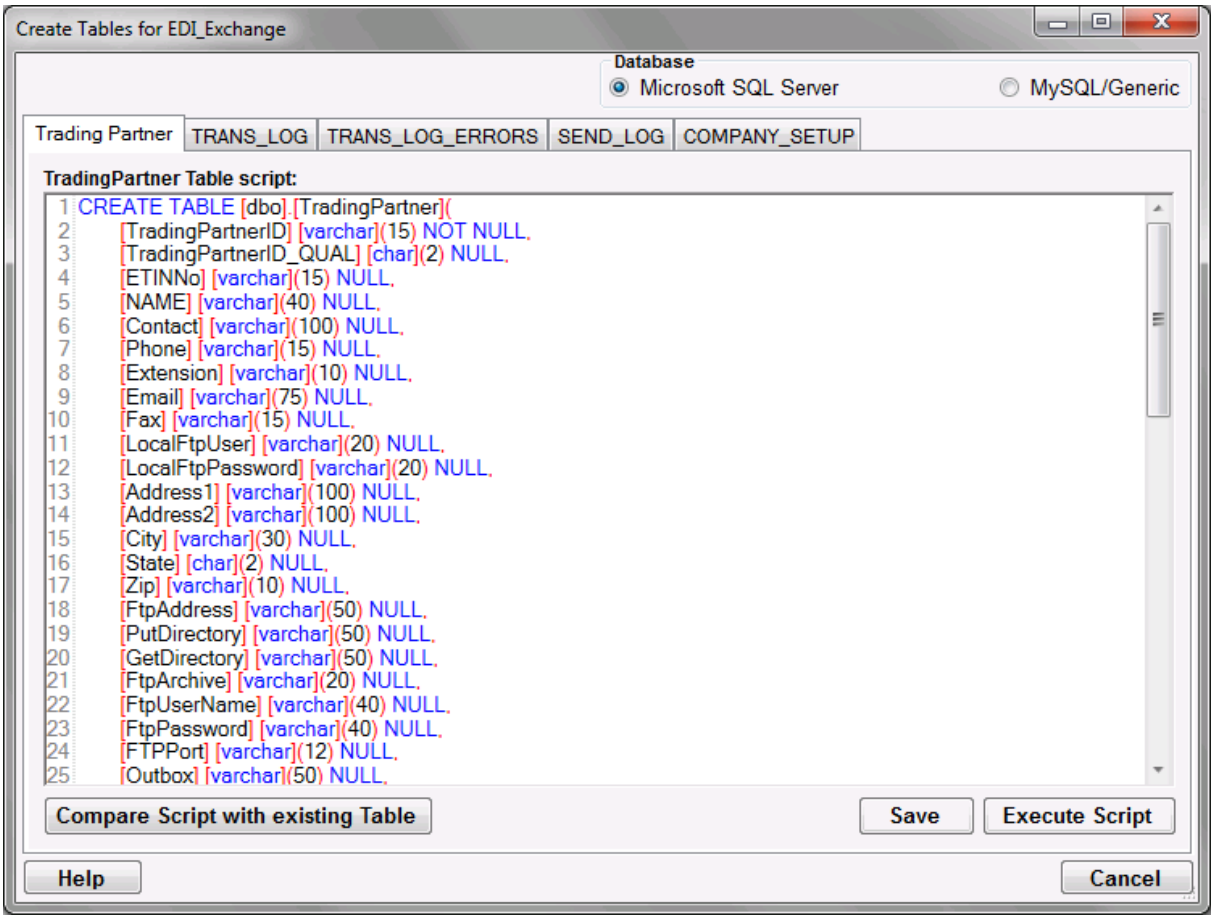
Once you have configured the database connection (Setting up Database Connection), follow the instructions below.

1. Select *EDI Exchange ▸ Create EDI Exchange Tables* in the main menu.



The menu item to create the necessary tables.

2. The "Create Tables for EDI_Exchange" screen will appear. Table creation and/or modification for your database is handled here.



The screen to create the tables

3. Select the database type you use for your host HIPAA application.
   - **Database**
     - **Microsoft SQL Server** (SQL Server 2008 and above)
     - **MySQL**

   Note: In case your database is not listed, modify the scripts or ask your database administrator to make the necessary modifications.

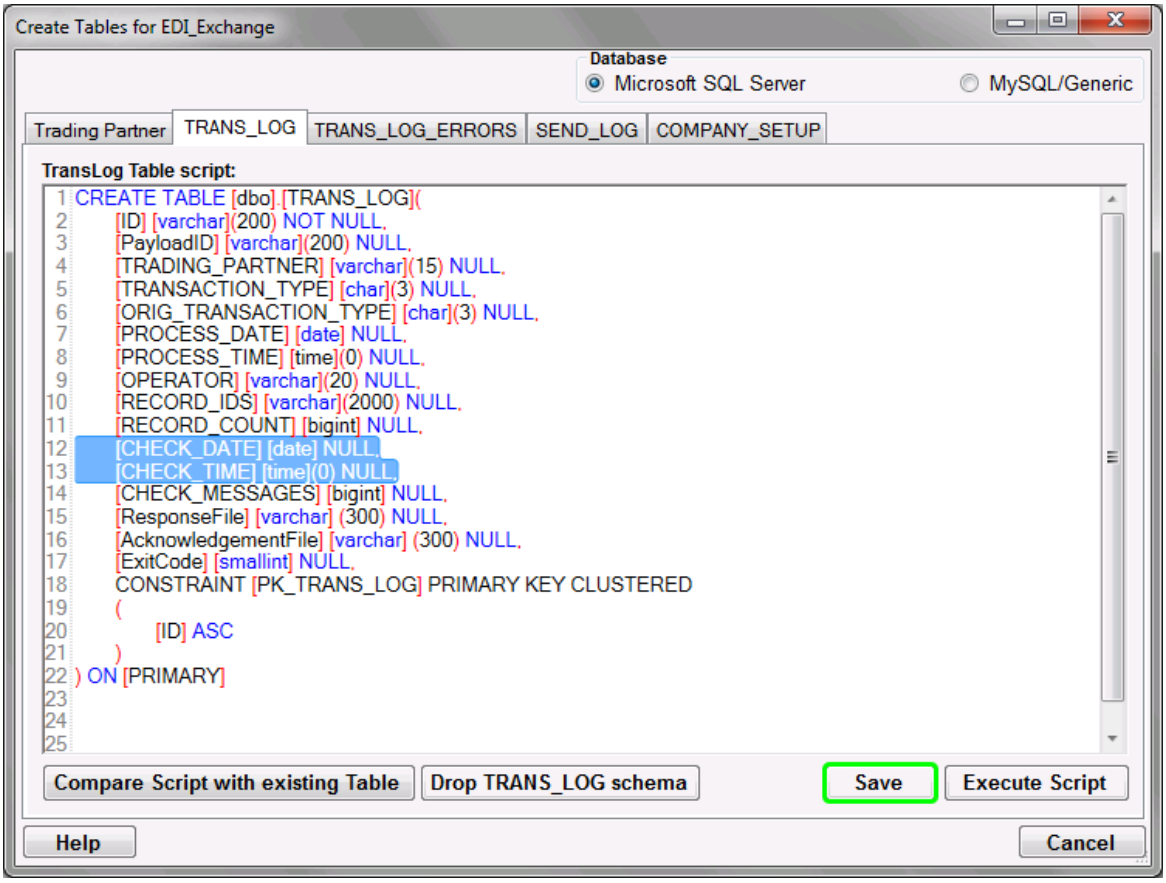
4. The following tables are part of EDI Exchange:
   - **TradingPartner** — SQL statements to create the "TradingPartner" table in your database. This table contains information about trading partners.
   - **Trans_Log** — SQL statements to create the "TRANS_LOG" table in your database. This table contains incoming file information, keeps track of all EDI files that you receive and the compliance check report.
   - **Trans_Log_Errors** — SQL statements to create the "TRANS_LOG_ERRORS" table in

your database. This table collects the results of the compliance check and keeps track of all sent files.

- **Send_Log** – SQL statements to create the "SEND_LOG" table in your database. The table contains information about EDI files created and sent to trading partners.
- **Company_Setup** – SQL statements to create the "COMPANY_SETUP" table in your database. This table collects information about you, the sender of EDI information.

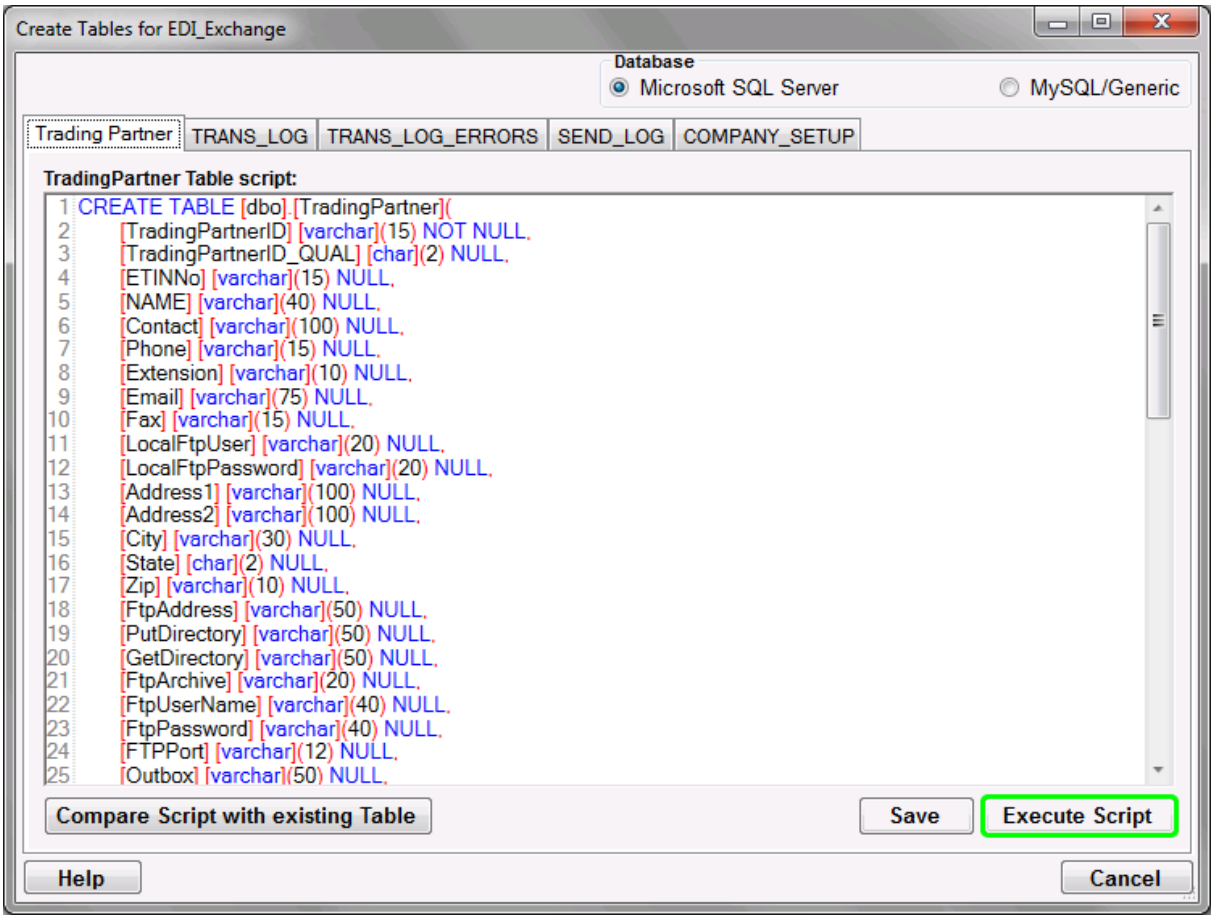
5. You can modify the scripts so that they run on your specific database. Once you have you modified the script, click "Save."

> Tip: Every database system has their own little syntax idiosyncrasies and the scripts might require tweaking. You can edit the table scripts in this screen and save your modified scripts. One example are 'date' and 'time' or 'money' data types that do not exist in SQL Server 2005. You can just rename those types to 'datetime' and save you script and it will run fine.



The "Save" button

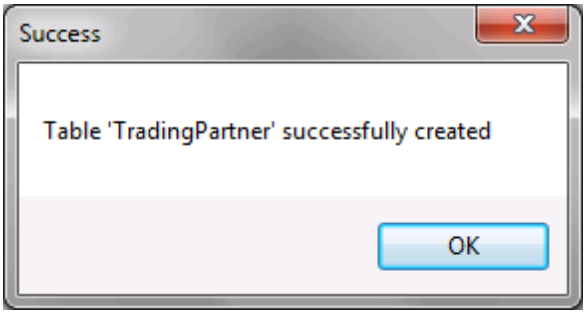
6. For **each** script on every tab, click "Execute Script" to create the corresponding table in the database.



The "Execute Script" button

> Notice: Creating tables means clicking the "Execute Script" button in all five tabs of the "Create Tables for EDI_Exchange" window. Then close this window.

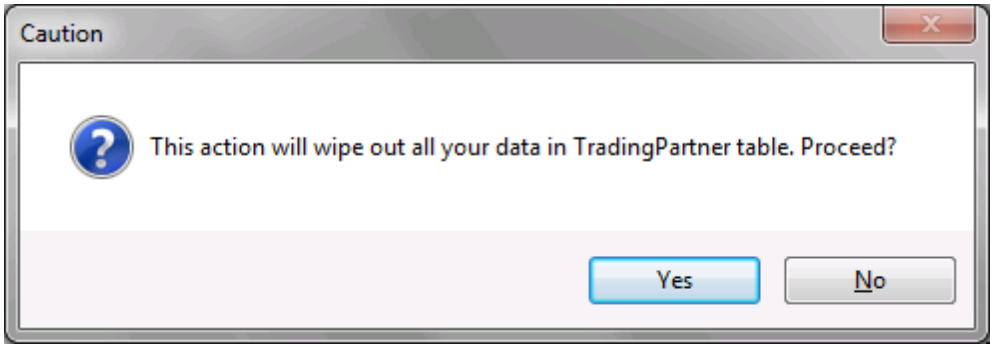
7. Once the table has been created successfully, you will see the following notification:



The Create Table script success message

> **Warning: Double-execution of a script wipes out the previous table you have created. A prompt will warn you before deleting an existing table. To Add/Remove fields use the "Compare Script..." button. Remove the script files once you have created the tables so nobody can destroy the tables**

by accident.



The double-execution warning message.

Make sure there are no error messages and the table creation has been completed successfully.

Compare Script with existing Table

HIPAAsuite products go through continual development and improvements. Often these changes lead to new fields in the database. While it is easy to drop a table and regenerate it with the new fields, you will loose all the data in the table. To avoid this trouble there is the button "Compare Script with existing Table". I you click this, the table structure in your database will be compared with the script. There are two possible outcomes. Your table is up to date

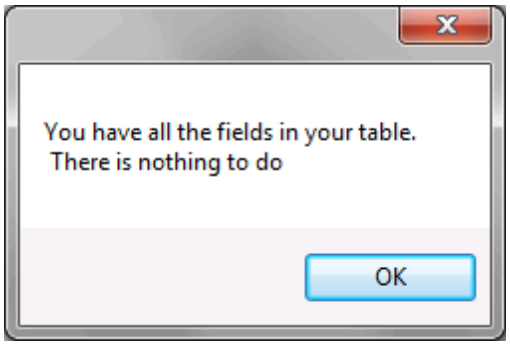
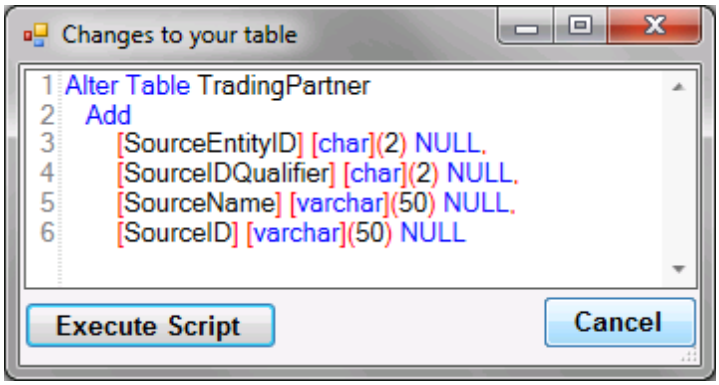


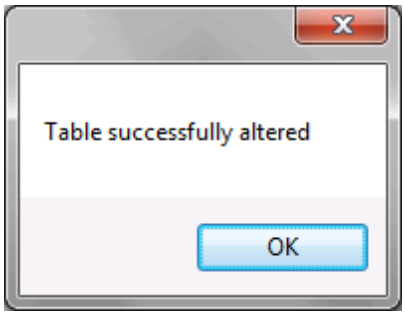
Table is up to date

or if your table is missing recently added fields, you will see a window pop up that shows an 'Alter Table' script with which you can add those fields to the table without interfering with existing data.



The 'Alter Table' script that shows as a result of missing fields

You can now click the "Execute Script" button and the field will be added and a message will confirm your changes



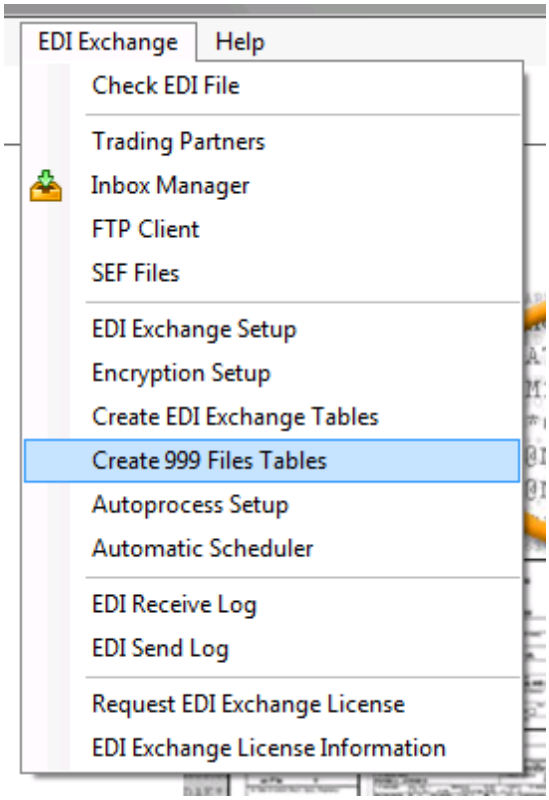
Alter Table statement successfully executed.

Once you have created the tables, you can start setting up the other application options. See the next step: Defining Auto-Processing Options.

9.2.3 2b Creating 999 File Tables

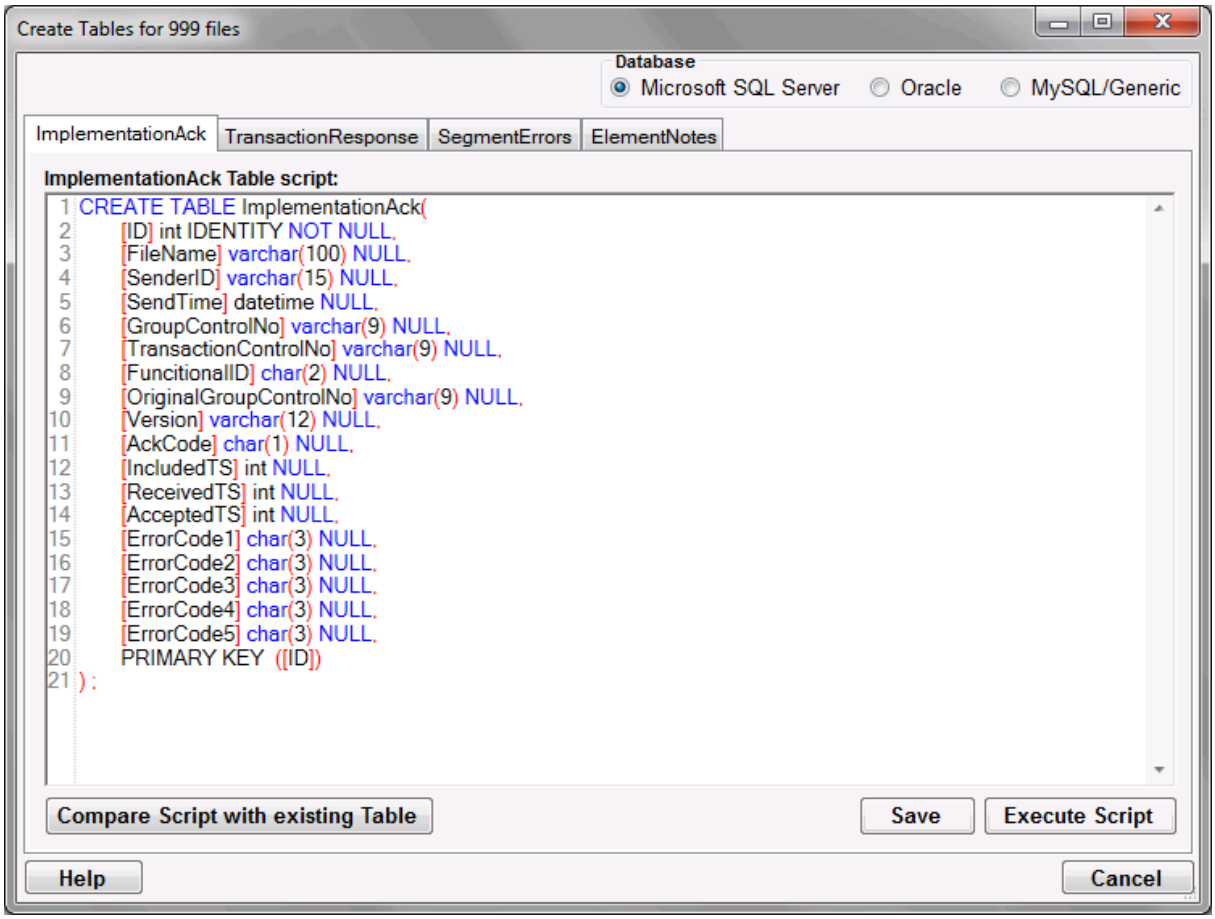
Once you have configured the database connection (Setting up Database Connection), follow the instructions below.

1. Select *EDI Exchange* ▸ *Create 999 Files Tables* in the main menu.



The menu item to create the necessary tables

2. The "Create Tables for 999 Files" screen will appear. Table creation and/or modification for your database is handled here.



The screen to create the tables

3. Select the database type you use for your host HIPAA application.

- **Database**
  - **Microsoft SQL Server** (SQL Server 2008 and above)
  - **Oracle**
  - **MySQL**

> Note: In case your database is not listed, modify the scripts or ask your database administrator to make the necessary modifications.

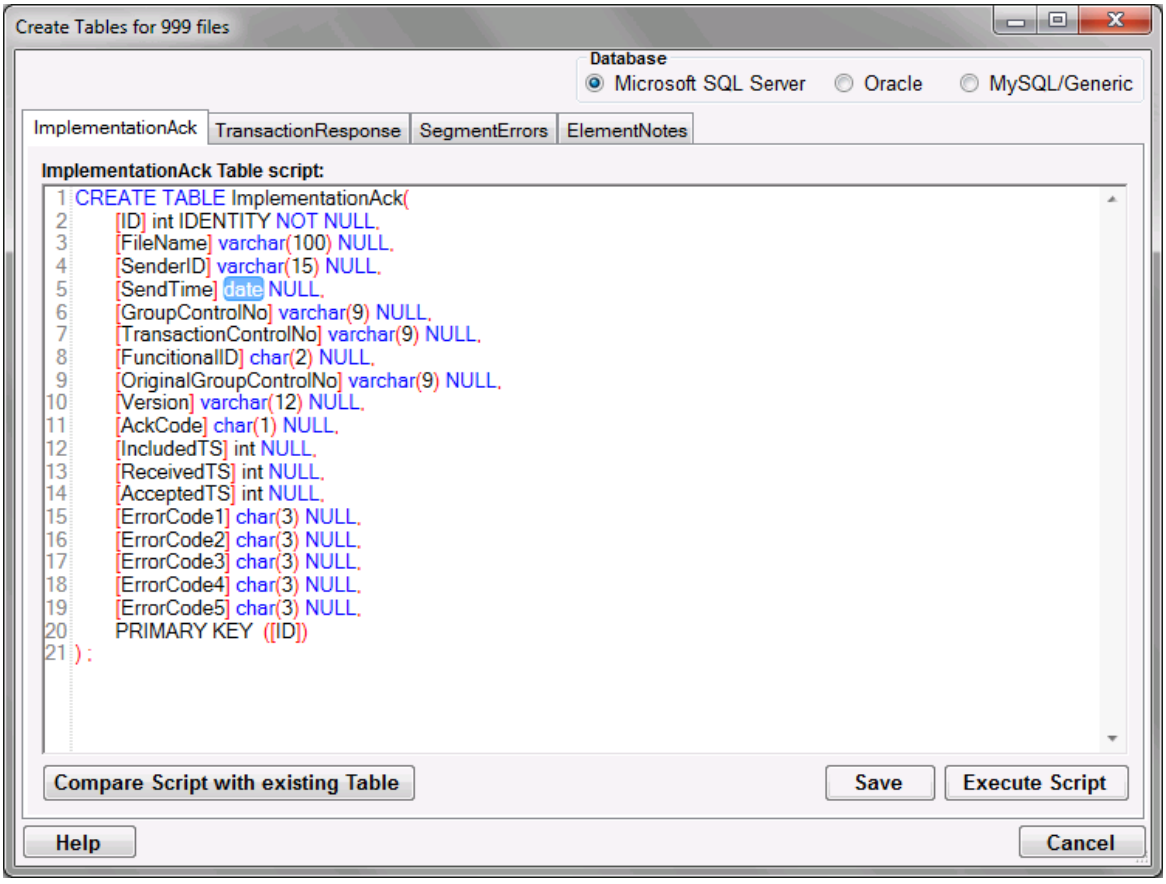
1. The following tables are part of EDI Exchange:

- **ImplementationAck** — SQL statements to create the "ImplementationAck" table in your database. This table contains information about Acknowledgments.
- **TransactionResponse** — SQL statements to create the "TransactionResponse" table in your database. This table contains individual transactions contained in 999 files.

- **SegmentErrors** — SQL statements to create the "SegmentErrors" table in your database. This table contains individual segments in error contained in 999 transactions.
- **ElementNotes** — SQL statements to create the "ElementNotes" table in your database. The table contains the elements in error in a specific segment.

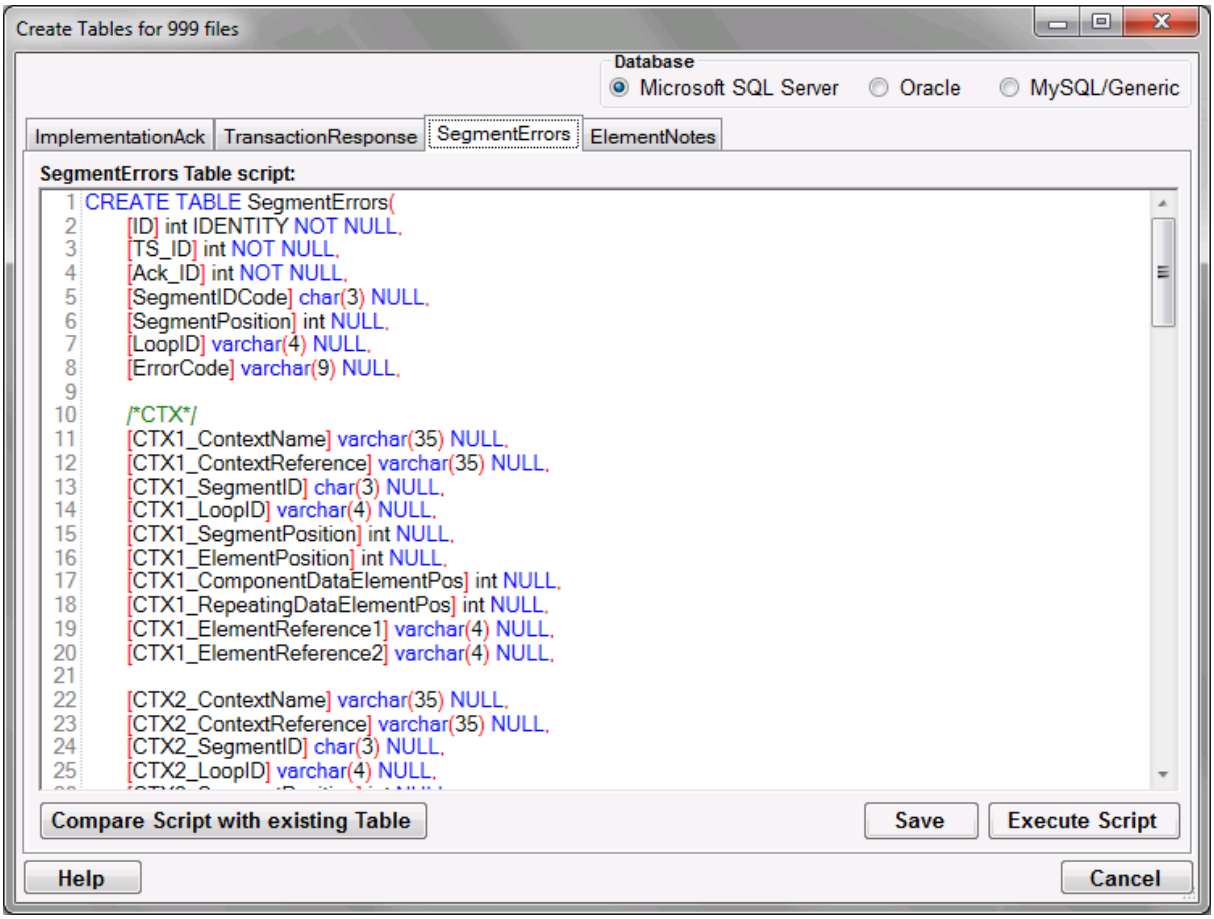
5. You can modify the scripts so that they run on your specific database. Once you have you modified the script, click "Save."

> Tip: Every database system has their own little syntax idiosyncrasies and the scripts might require tweaking. You can edit the table scripts in this screen and save your modified scripts. One example are 'date' and 'time' or 'money' data types that do not exist in SQL Server 2005. You can just rename those types to 'datetime' and save you script and it will run fine.



The "Save" button

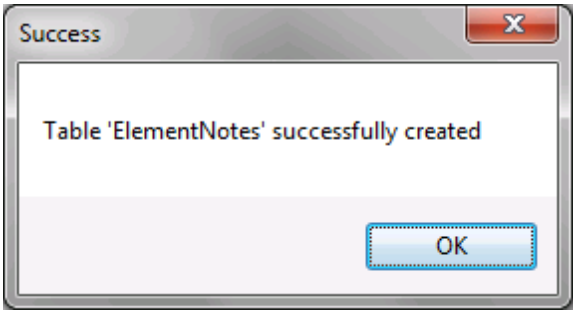
6. For **each** script on every tab, click "Execute Script" to create the corresponding table in the database.



The "Execute Script" button

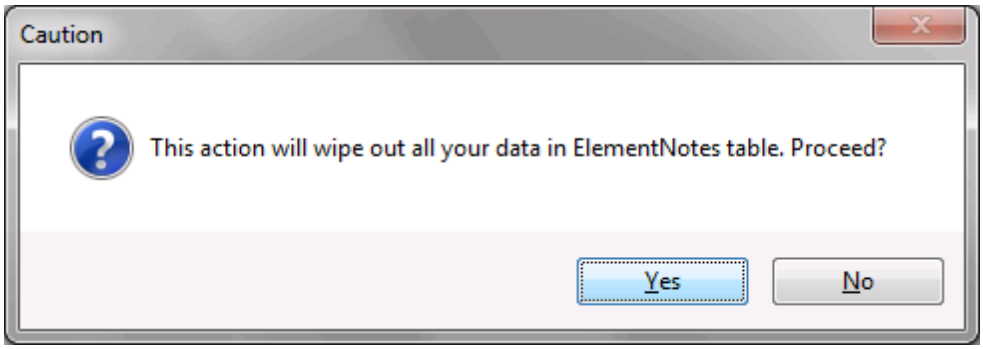
> Notice: Creating tables means clicking the "Execute Script" button in all four tabs of the "Create Tables for 999 Files" window. Then close this window.

7. Once the table has been created successfully, you will see the following notification:



The Create Table script success message

> **Warning: Double-execution of a script wipes out the previous table you have created. A prompt will warn you before deleting an existing table. To Add/Remove fields use the "Compare Script..." button. Remove the script files once you have created the tables so nobody can destroy the tables by accident.**



The double-execution warning message.

Make sure there are no error messages and the table creation has been completed successfully.

Compare Script with existing Table

HIPAAsuite products go through continual development and improvements. Often these changes lead to new fields in the database. While it is easy to drop a table and regenerate it with the new fields, you will loose all the data in the table. To avoid this trouble there is the button "Compare Script with existing Table". I you click this, the table structure in your database will be compared with the script. There are two possible outcomes. Your table is up to date

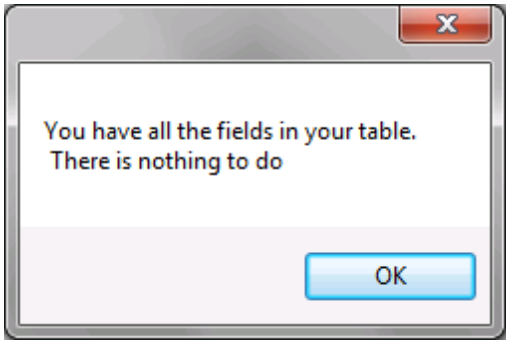
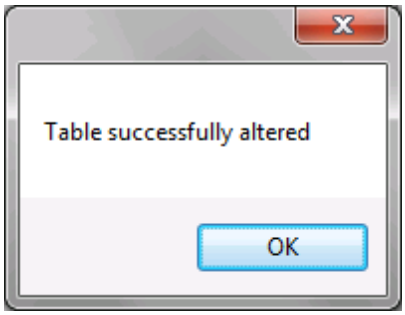


Table is up to date

or if your table is missing recently added fields, you will see a window pop up that shows an 'Alter Table' script with which you can add those fields to the table without interfering with existing data. In the latter case, you can click the "Execute Script" button and the field will be added and a message will confirm your changes

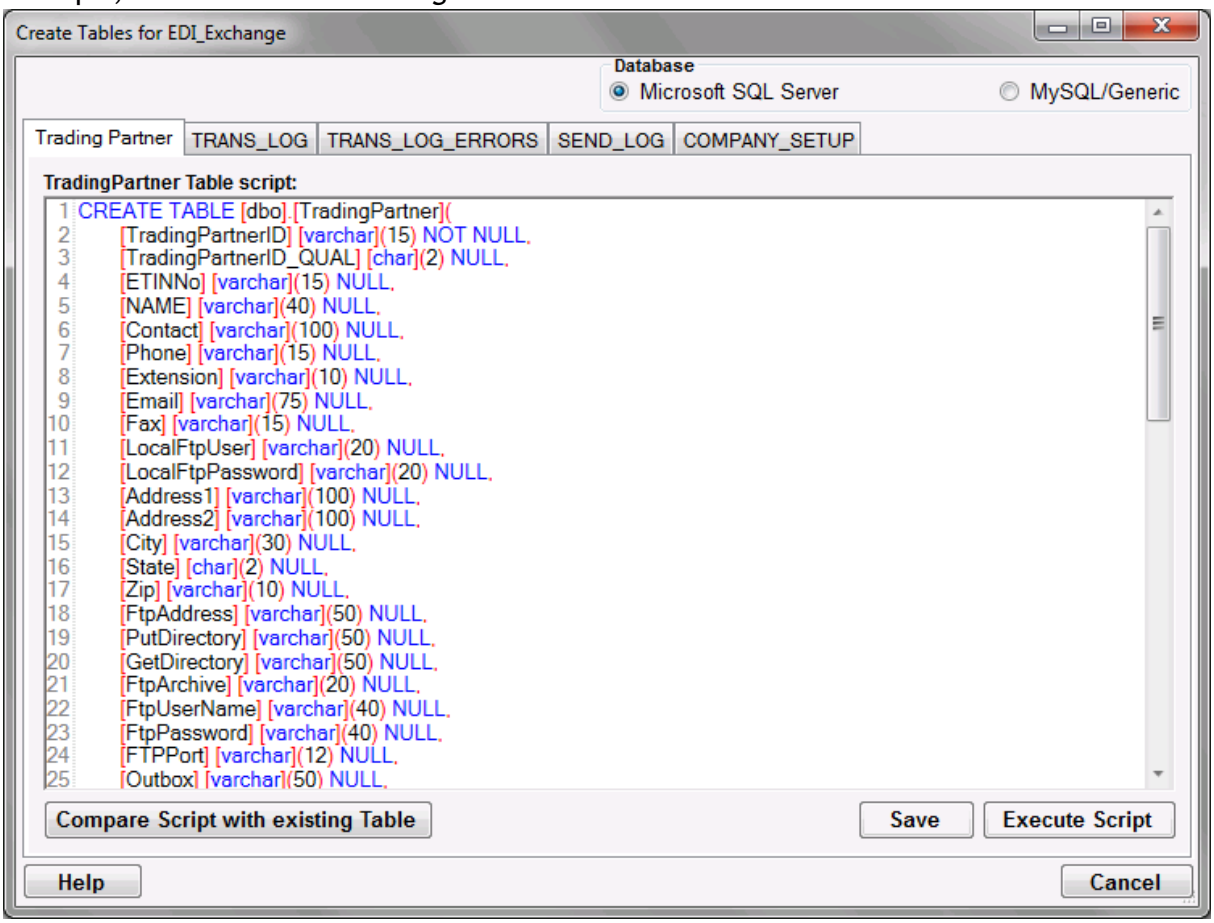


Alter Table statement successfully executed.

9.2.4 2c Updating Database Tables

To update an existing table (in the event of an update, for example), follow the instructions below.

1. Start with the table creation script window of the table you want to update. In this example, we will use the *Trading Partner* table.



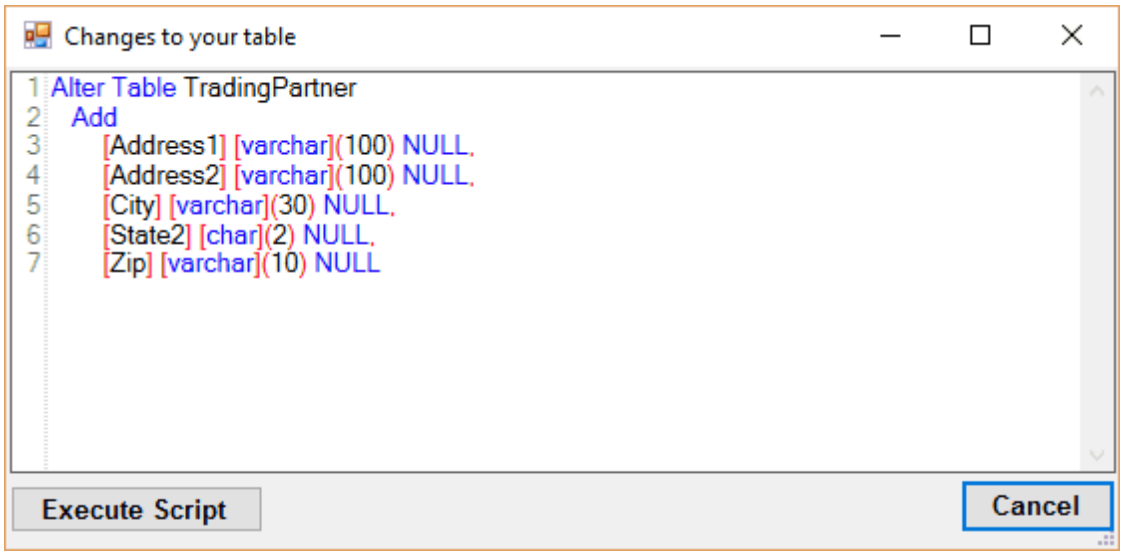
The table creation script for the Trading Partner table.

2. In the case of modifying a table to include/exclude/change a field or fields required by

a program update, the script will have been updated for you and clicking the *Compare Script with existing Table* button will bring you to the next step. To modify the table yourself in order to conform to your particular database, first edit the script text to suit your database system, click the *Save* button, then the *Compare Script with existing Table* button, and proceed to the next step.

> Tip: Every database system has their own little syntax idiosyncrasies and the scripts might require tweaking. You can edit the table scripts in this screen and save your modified scripts. One example are 'date' and 'time' or 'money' data types that do not exist in SQL Server 2005. You can just rename those types to 'datetime' and save you script and it will run fine.

3. Having clicked *Compare Script with existing Table*, the script will be compared to the existing table and any additional fields will be presented. In this example, the Trading Partner table's Address fields will be added.



Changes to be made to Trading Partner table.

4. Click *Execute Scipt*. This will perform the additions/changes stated in the alter table script and a prompt will appear informing you of the change. The table has now been modified.

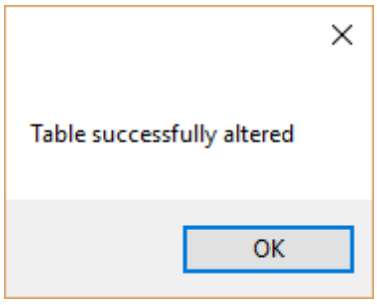


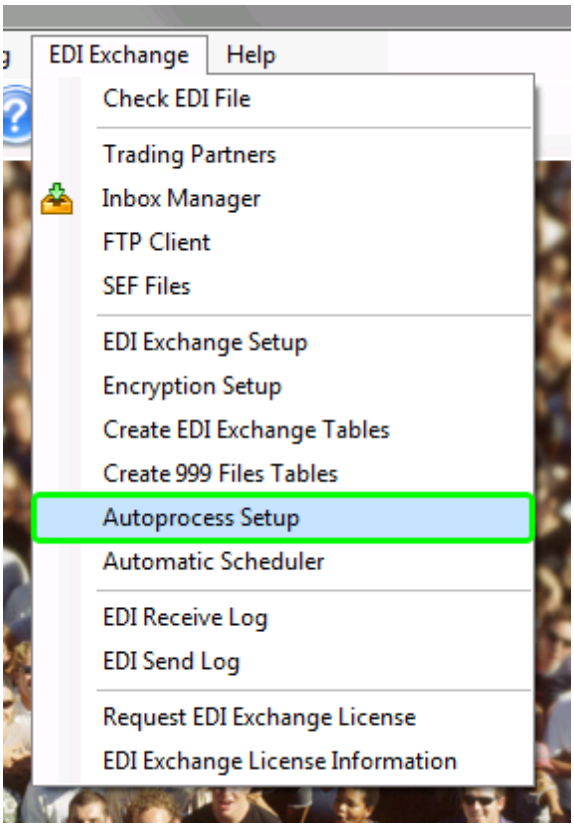
Table has been altered.

9.2.5 3 Defining Auto-Processing Options

In the "Auto-Process Setup" you can instruct the program on what to do after analyzing and decrypting the received files in the Inbox Manager. The auto processing enables you to combine and run multiple fulfillment steps together (for example, export, saving, printing.) These options are important for the hand-over from EDI Exchange to the other HIPAAsuite program that hosts EDI Exchange.

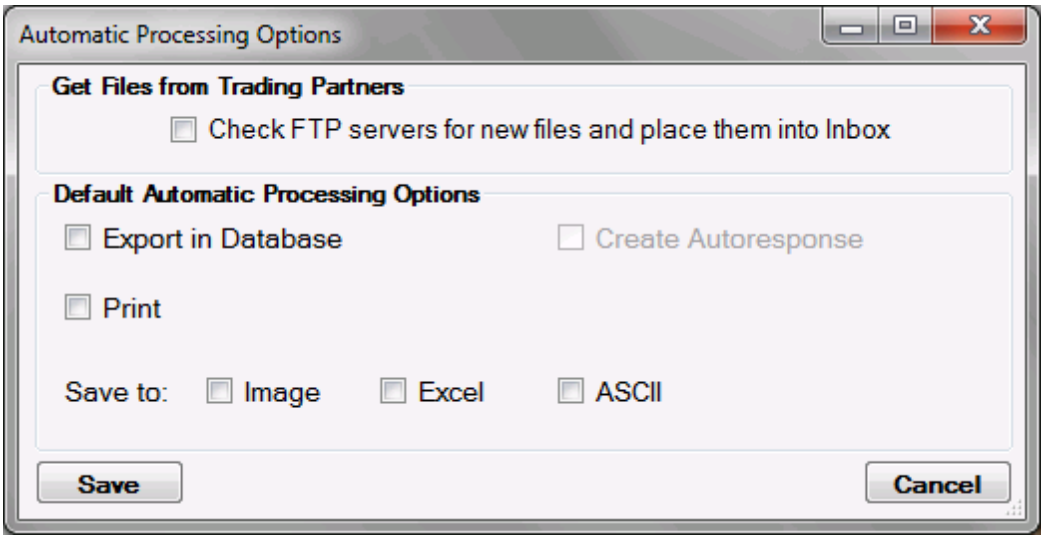
Follow the instructions below to specify the Auto Process Options.

1. Select *EDI Exchange* ▸ *Autoprocess Setup* in the main menu.



The "Autoprocess Setup" menu item

2. The following screen will appear if the host HIPAA application is Enrollment Master.



Defining the Auto Processing Options

3. The following options can be specified:

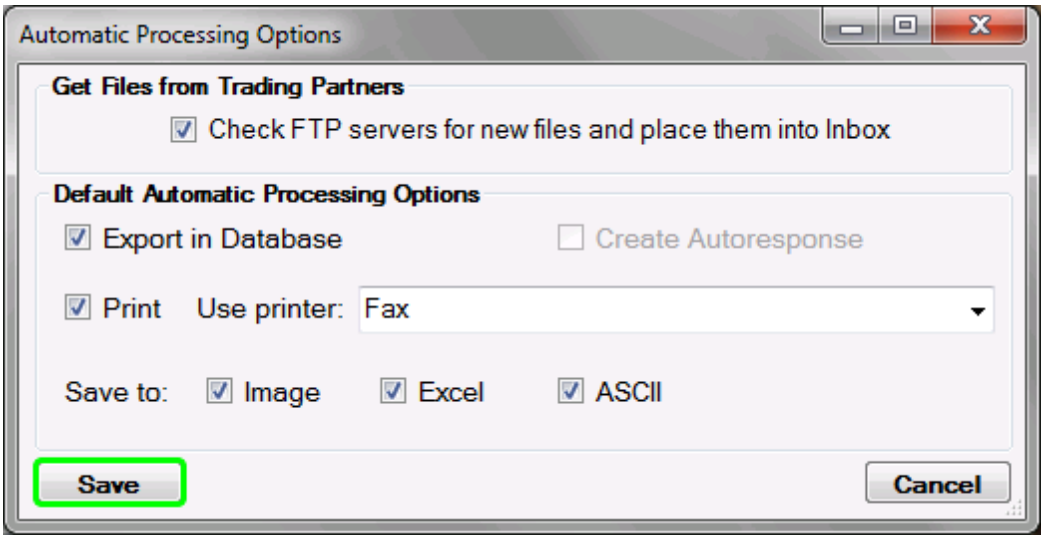
Check Path Options

- **Check FTP servers for new files** — If checked, EDI Exchange automatically looks for new files for all trading partners that have FTP connection set up. Then the program gets all the waiting files and puts them into the Inbox. In the second step, it goes through every file.

Default Automatic Processing Options

- **Export in Database** — If selected, the module exports new files to the database.
- **Print** — If selected, the module prints files using the selected printer.
- **Create Auto-Response** — If selected, the module creates an auto-response to the received files.
- **Save to** — If selected, the system automatically saves files as:
    - **Image**
    - **Excel**
    - **ASCII**

4. Click "Save."



The "Save" button

Once you have saved the auto-processing options, the files will not only be analyzed but also processed according to the defined settings. Proceed to the next step: Defining Communications Directory.

9.2.6 4 Defining Communications Directory

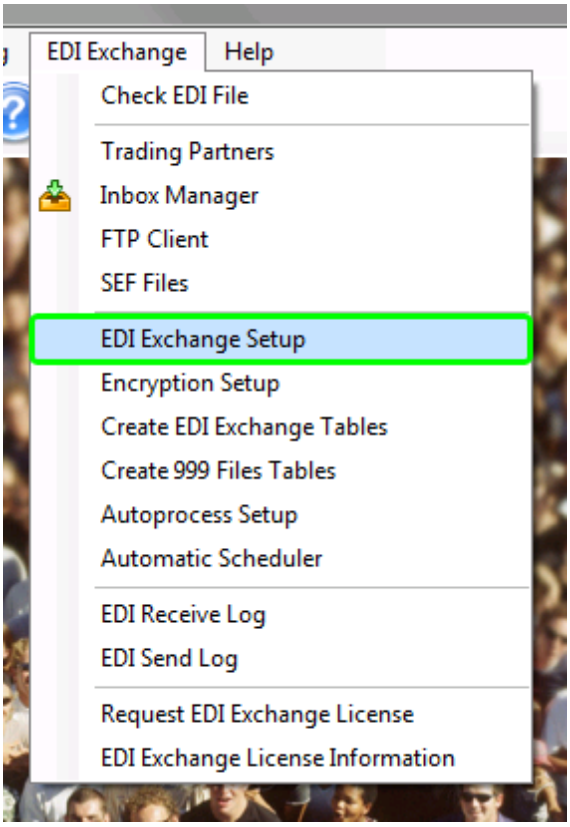
EDI file directory is an obligatory setting you need to set up before starting using the EDI Exchange. In order to keep track of the thousands of EDI files that accumulate over time, EDI Exchange uses a folder structure which we call the "HIPAAsuite Communications Directory" or "HIPAAsuiteCommDir" in short. In it, you will find all your EDI files sorted into several categories:

- **Inbox**
- **Outbox**
- **ProcessedFiles**
- **EncryptedFiles**
- **SuspendedFiles**

Within these directories, there will be folders for each Trading Partner and type of transaction. The location and names of the sub-folders are handled in the "Trading Partner Setup." See Setting up Trading Partners.

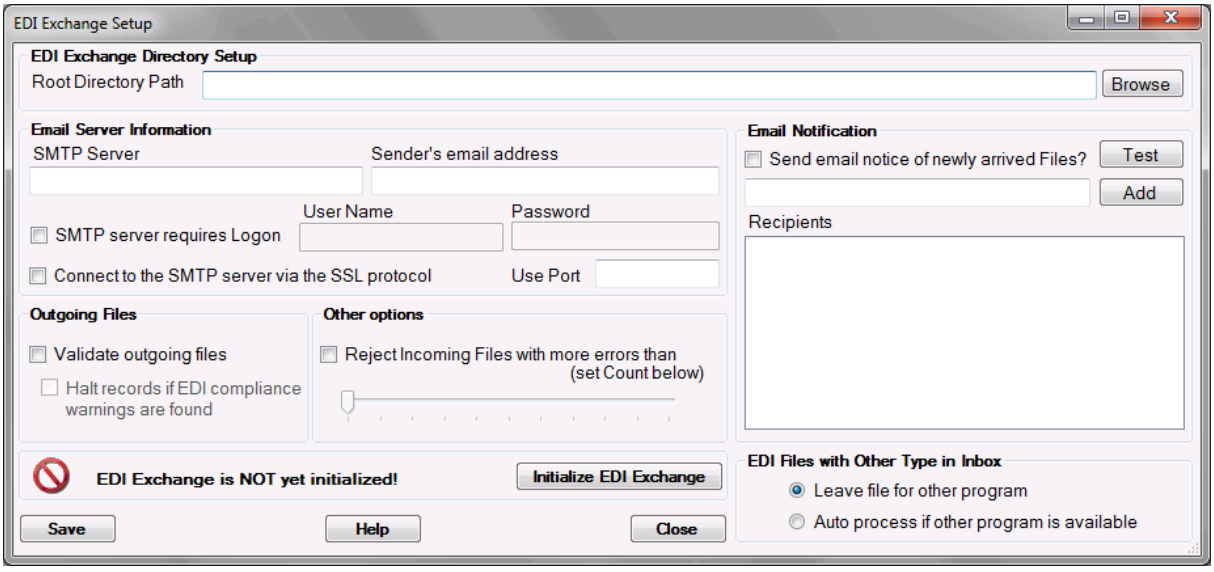
Follow the instructions below to specify EDI communications root directory.

1. Select "EDI Exchange Setup" under the "EDI Exchange" menu item.



The "EDI Exchange Setup" menu item

2. The following window will appear.

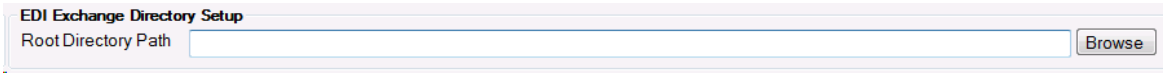


The "EDI Exchange Setup" window

> Note: The icon in the lower left corner indicates that EDI Exchange has not been initialized yet.

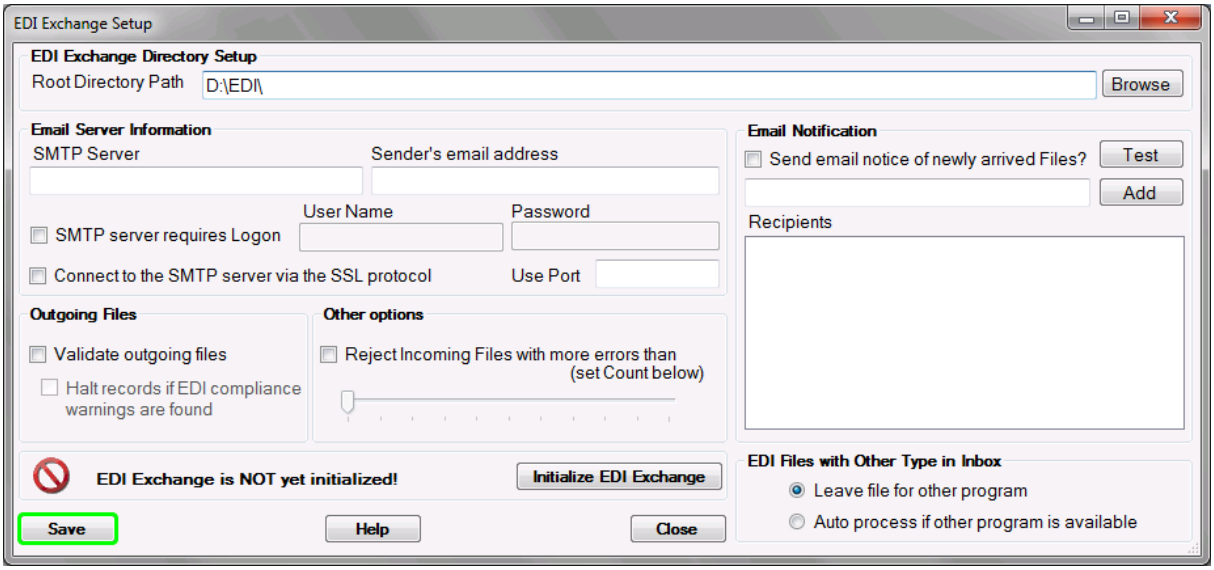
3. Under "EDI Exchange Directory Setup" specify the following setting:

- **Root Directory Path** — Define the root path in the "Root Directory Path" text field. The root path is the folder where all your EDI files reside. EDI Exchange will later create sub-directories required to operate.



The root communications directory setup

4. Click "Save."



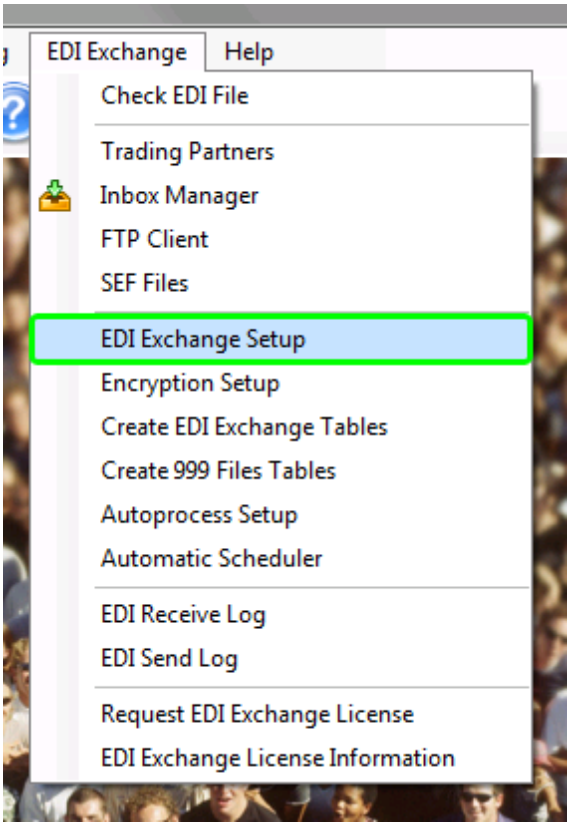
The "Save" button

After setting the root directory, you can click the "Initialize EDI Exchange" button. Read more in Initializing EDI Exchange.

9.2.7 5 Initializing EDI Exchange

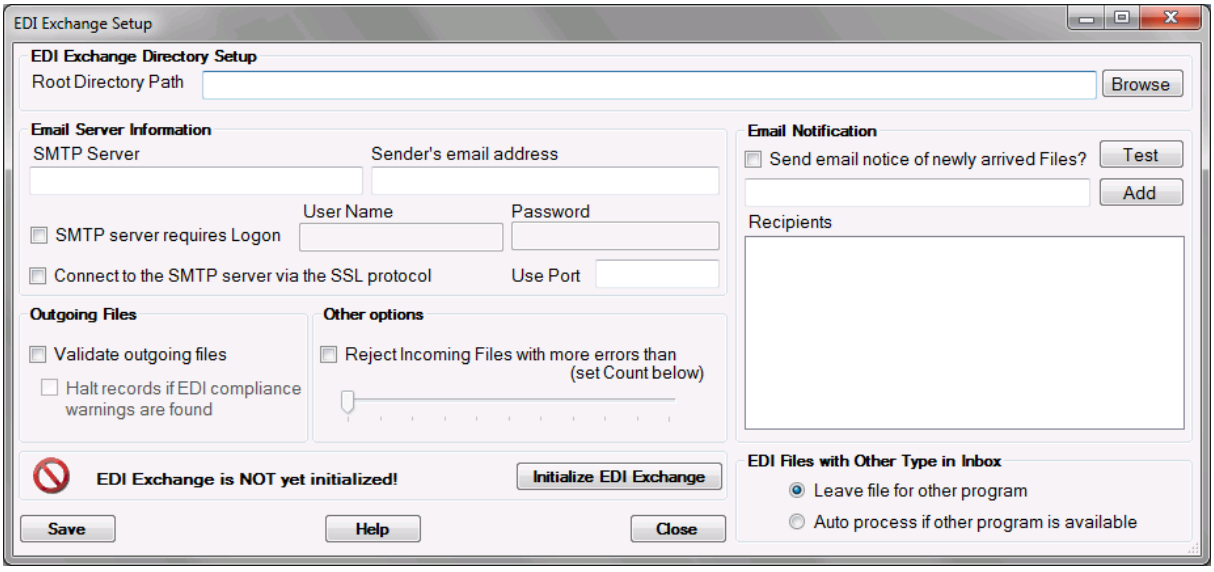
Before you can use EDI Exchange, and after you have configured the obligatory settings, you have to perform the initialization. Follow the instructions below.

1. Select "EDI Exchange Setup" under the "EDI Exchange" menu item.



The "EDI Exchange Setup" menu item

2. The following window will appear.

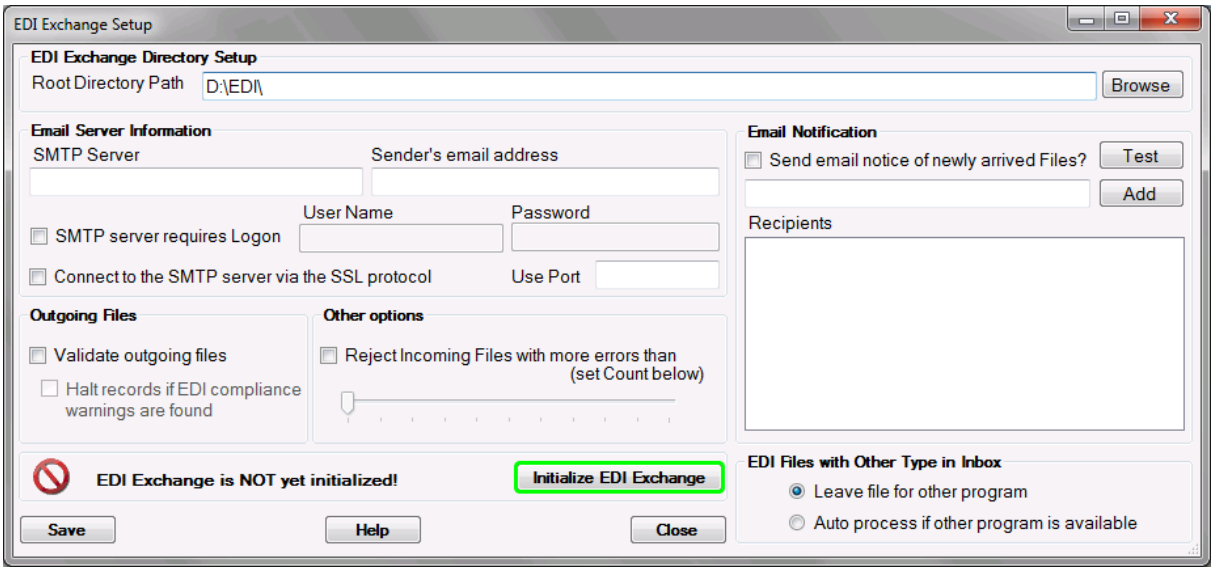


The "EDI Exchange Setup" window

> Note: The icon in the lower left corner, indicating that EDI Exchange has not been initialized yet.

3. After setting the root directory (see the previous step Defining Communications

Directory), you can initialize EDI Exchange module. Click the "Initialize EDI Exchange" button to accomplish the process.



The "Initialize EDI Exchange" button

Once the "Initialize EDI Exchange" button is clicked, the system checks if all settings have been configured correctly.

1. The first thing the initialization process checks is the connection to the database and the presence of the necessary tables. EDI Exchange relies on the database connection that is part of the HIPAAsuite application that you are using. EDI Exchange needs Database Connectivity licensed and enabled. If this part is not yet set up, then you will get an error like this:

Initialization failed because of SQL connection problems

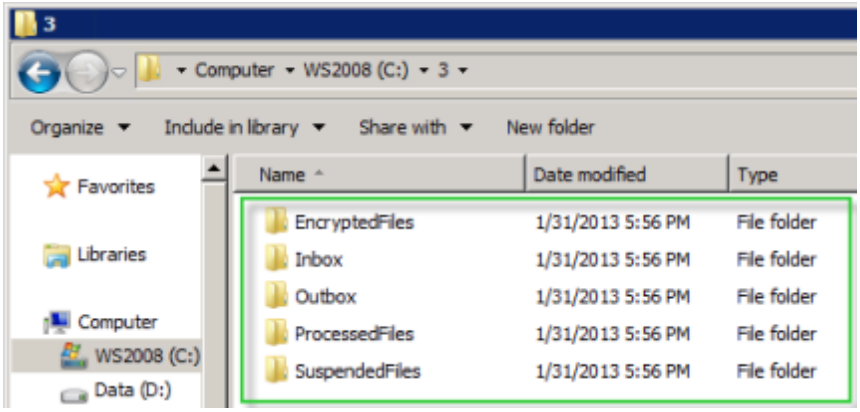
Read more in Setting up Database Connection.

2. Once the connection is established, the program checks if the correct tables exist in the database. See Creating Database Tables. Once the SQL part checks out, you will see the following message.

```
Checking SQL settings and tables:
          Connection settings are checked. Trading Partners table is checked.
          TRANS_LOG table is checked.
          TRANS_LOG_ERRORS table is checked.
          SEND_LOG table is checked.
```

3. The next step of the initialization processes — the program checks and, if necessary, creates the root directory and five sub-directories. Within these root directories, there will be folders for each Trading Partner and type of transactions. The location and names of the sub-folders are handled in the "Trading Partner" setup. The root folder is specified via the "EDI Exchange Setup" screen. Read more in Defining Root Directory.

   The sub-directories that EDI Exchange creates are as follows:

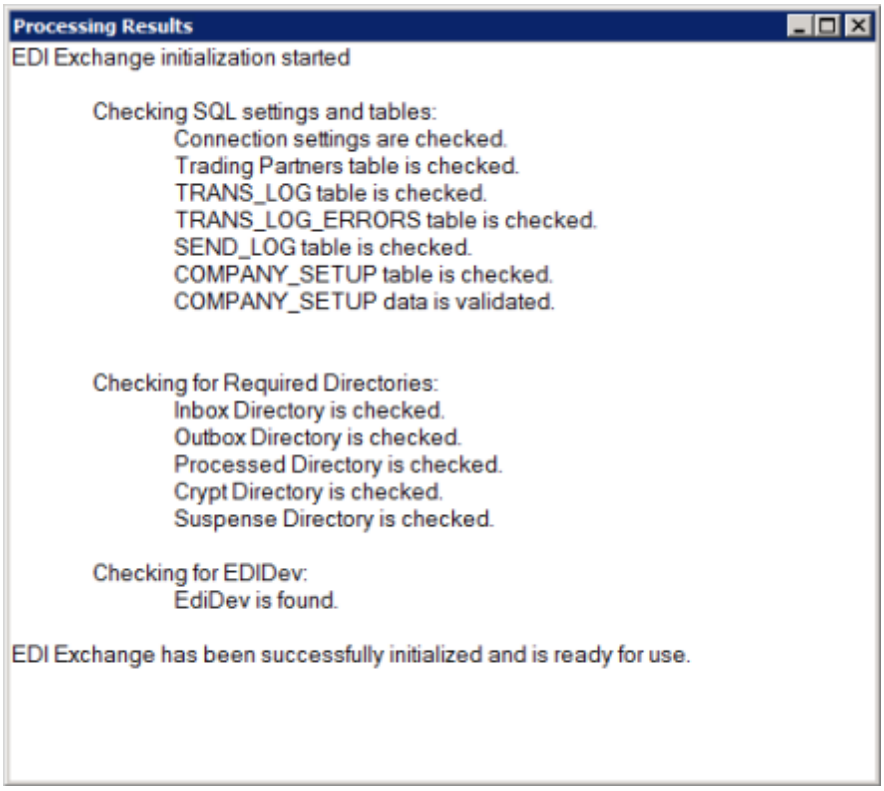


The directory structure of EDI Exchange

4. The next step of the initialization — the program checks if the HIPAA EDI compliance engine is properly installed.

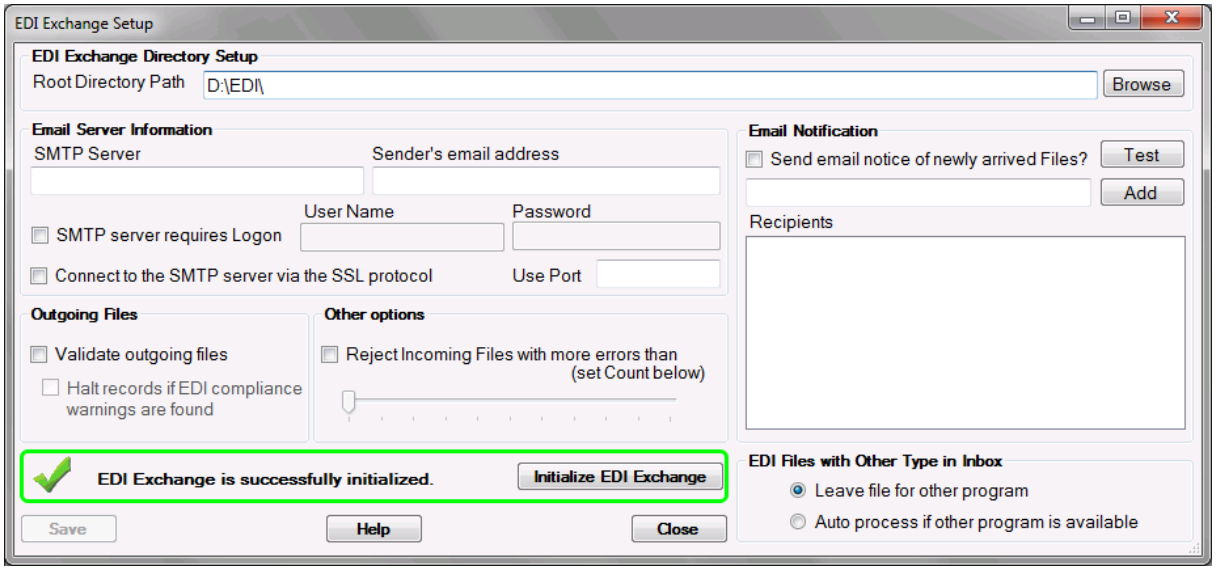
5. The last thing checked by the system is if the Automatic File Processing options have been set up. Read more in Defining Auto-Processing Options. The options are important for the hand over from EDI Exchange to the other HIPAAsuite program that hosts EDI Exchange.

Once all verifications have been completed successfully, you will see the following message:



Successful initialization of EDI Exchange

After that your EDI Exchange is initialized.



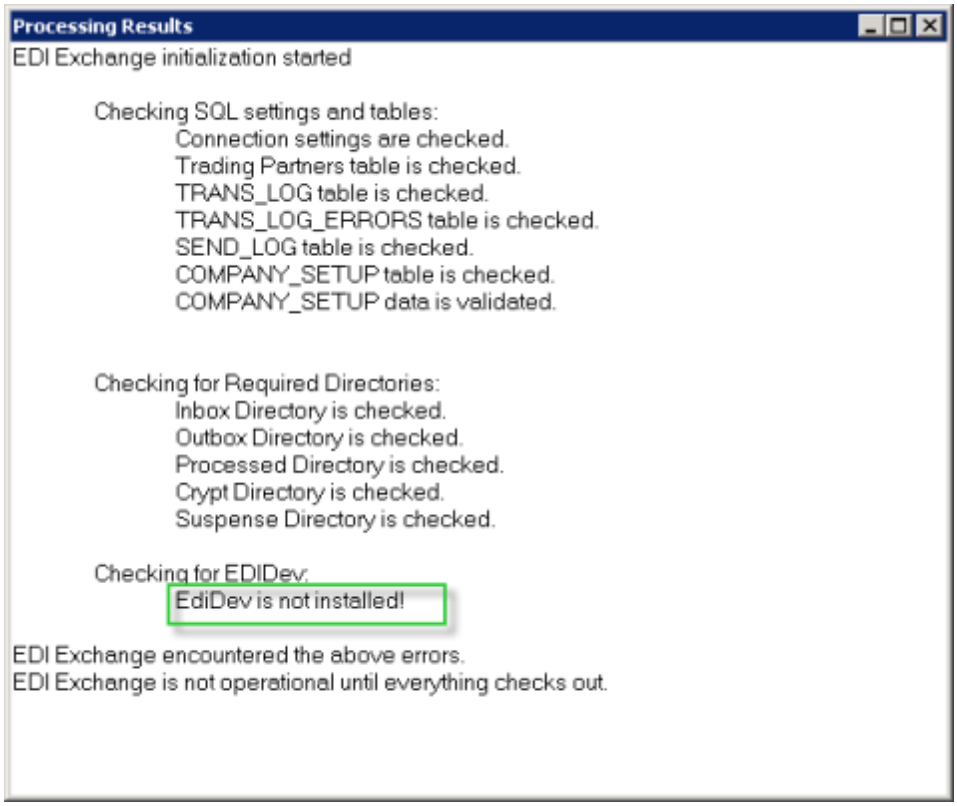
The "EDI Exchange is successfully initialized" message on the bottom of the "EDI Exchange Setup" window

Troubleshooting Initialization

When you are going through the Initialization process of the EDI Exchange, you can encounter the following message in the "Processing Results" window:

```
Checking for EDIDev:

EDIDev is not installed!
```

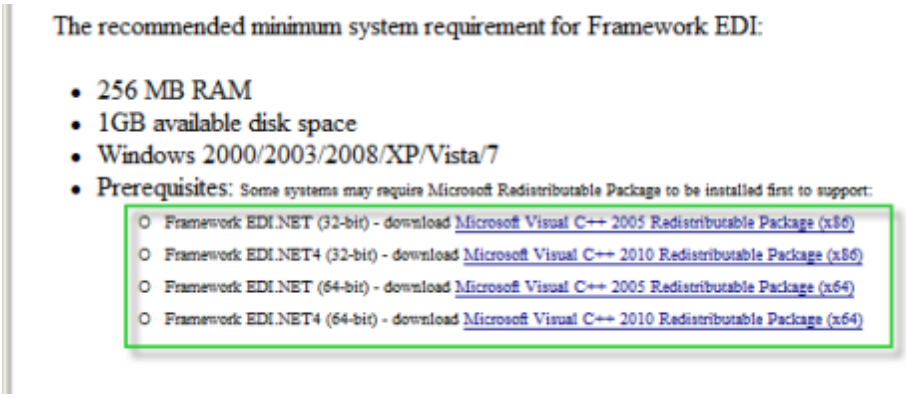


The EdiDev component is not installed

To resolve this issue, do the following.

1. Go to the http://www.edidev.com/ediregis.htm site.

2. Some systems may require Microsoft Redistributable Package to be installed first. In this case, download one of the following components according to your OS' bit depth.


The recommended minimum system requirement for Framework EDI:

- 256 MB RAM
- 1GB available disk space
- Windows 2000/2003/2008/XP/Vista/7
- Prerequisites: Some systems may require Microsoft Redistributable Package to be installed first to support:
  - Framework EDI.NET (32-bit) - download Microsoft Visual C++ 2005 Redistributable Package (x86)
  - Framework EDI.NET4 (32-bit) - download Microsoft Visual C++ 2010 Redistributable Package (x86)
  - Framework EDI.NET (64-bit) - download Microsoft Visual C++ 2005 Redistributable Package (x64)
  - Framework EDI.NET4 (64-bit) - download Microsoft Visual C++ 2010 Redistributable Package (x64)

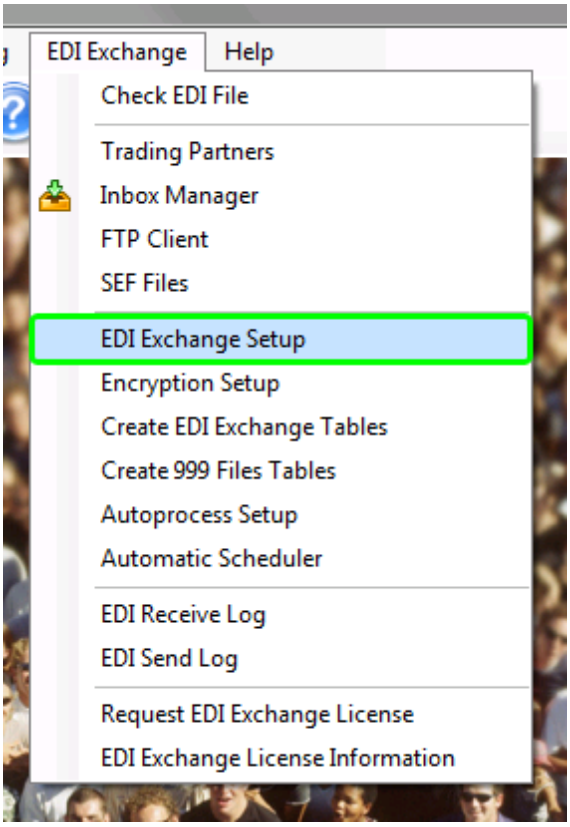
3. Download one of the following components you need according to your OS' bit depth:
   - Framework EDI Enterprise evaluation 32-bit
   - Framework EDI Professional evaluation 64-bit
4. Install downloaded components and start again the EDI Exchange initialization procedure.

9.3 Configuring EDI Exchange (Optional Settings)

9.3.1 Setting up Email Notifications

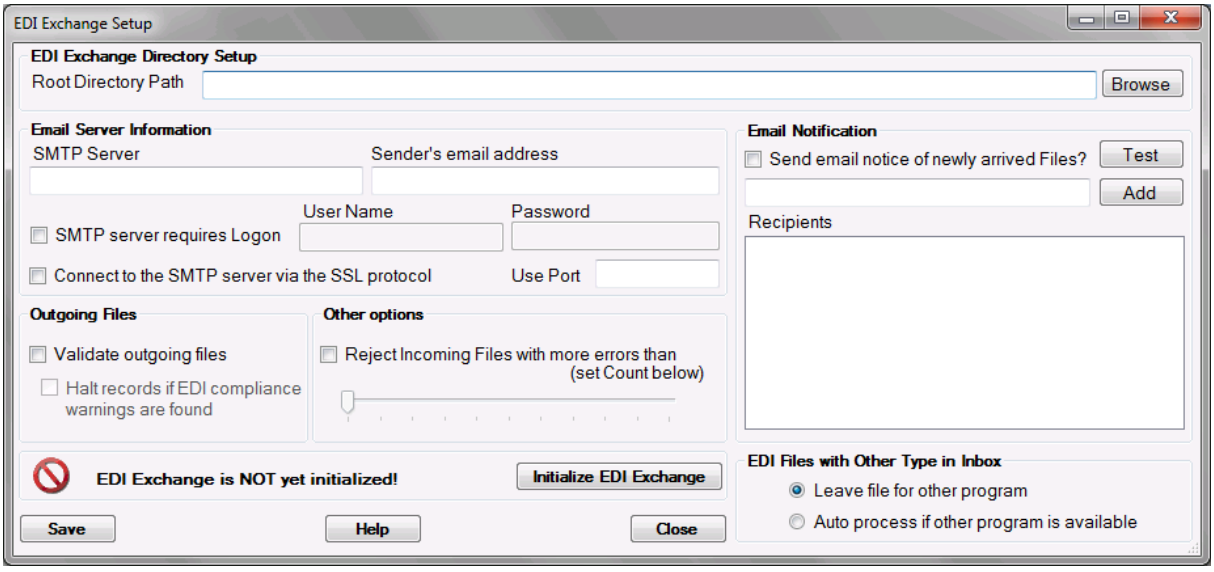
EDI Exchange can send emails to operators and trading partners to notify them about files and processing results. This functionality of EDI Exchange lies beyond the most basic setup that the initialization checks for. For this feature to work properly, you need to set up an email server which EDI Exchange communicates with. You can do this in the "Email Server Information" frame of the setup screen. Follow the instructions below.

1. Select "EDI Exchange Setup" under the "EDI Exchange" menu item.



The "EDI Exchange Setup" menu item

2. The following window will appear.

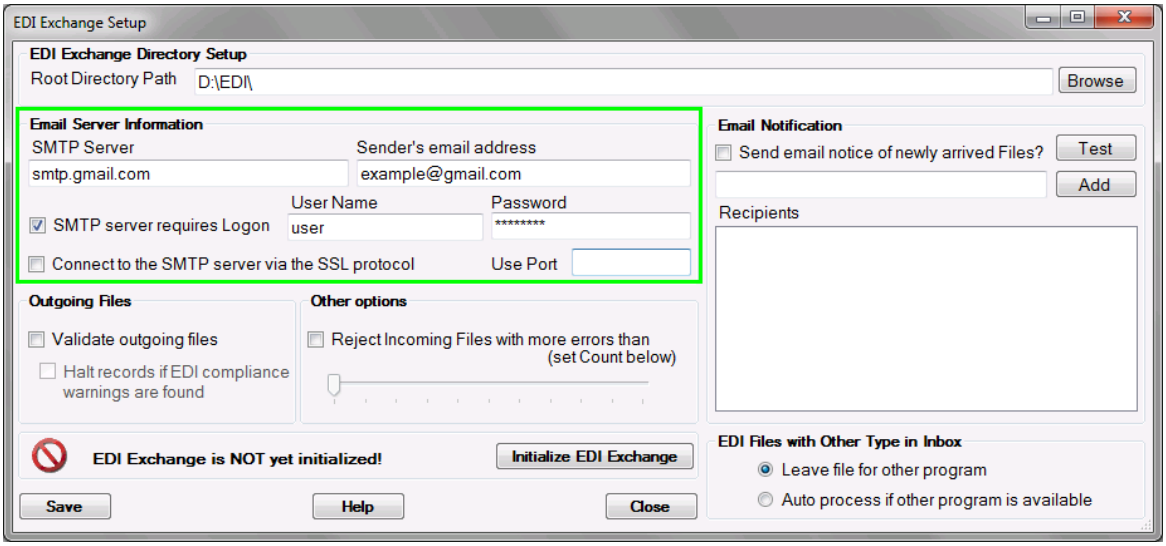


The "EDI Exchange Setup" window

3. Specify the following email options:

Email Server Information

- SMTP server
- Sender's email address
- SMTP server requires logon
- Username
- Password
- Connect to the SMTP server via the SSL protocol
- Use port



Setting up the email server

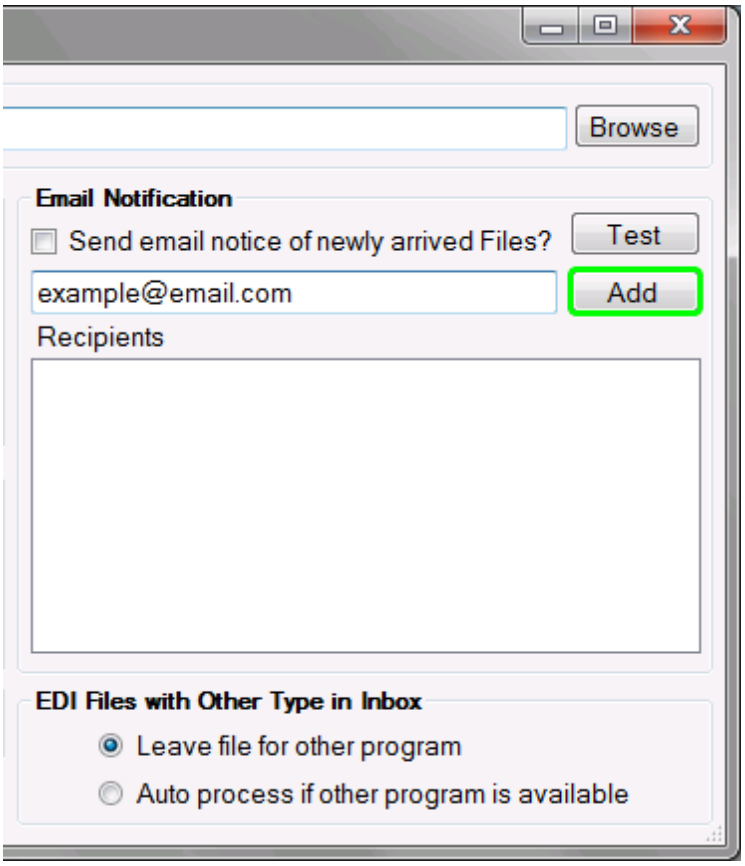
> Note: If you do not have this information, please ask your administrator to set this portion up for you.

4. To configure email notifications, specify the following options:

Email Notification

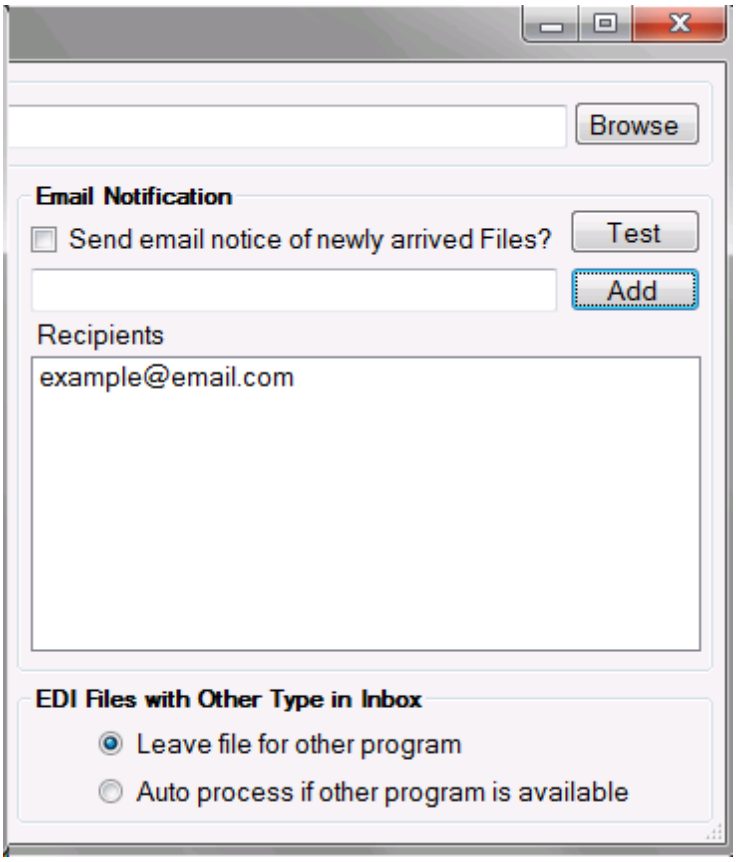
- **Send email notice of newly arrived files?** — Use this checkbox to define if you want to send email notice once new files have arrived.
- **Recipients** — You can add your staff's email(s) and the processing messages will be sent to these emails.

Enter an email address and click "Add."



Setting up the email recipients

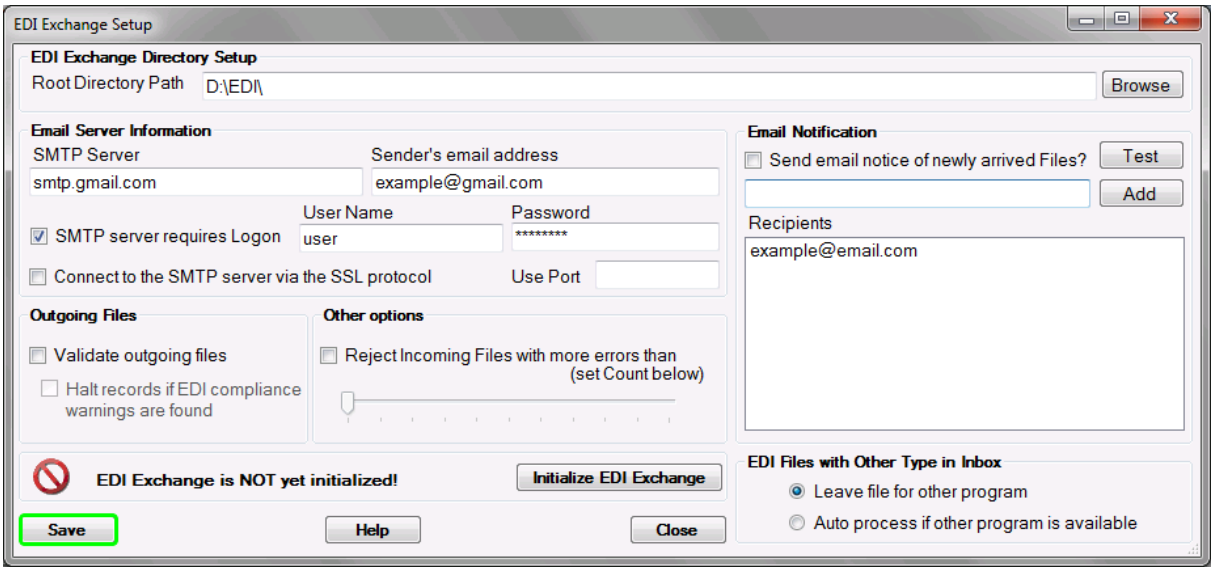
The email address will appear in the list.



Added email recipient

5. Click on the "Test" button to verify your settings.

6. Click on the "Save" button.



The "Save" button

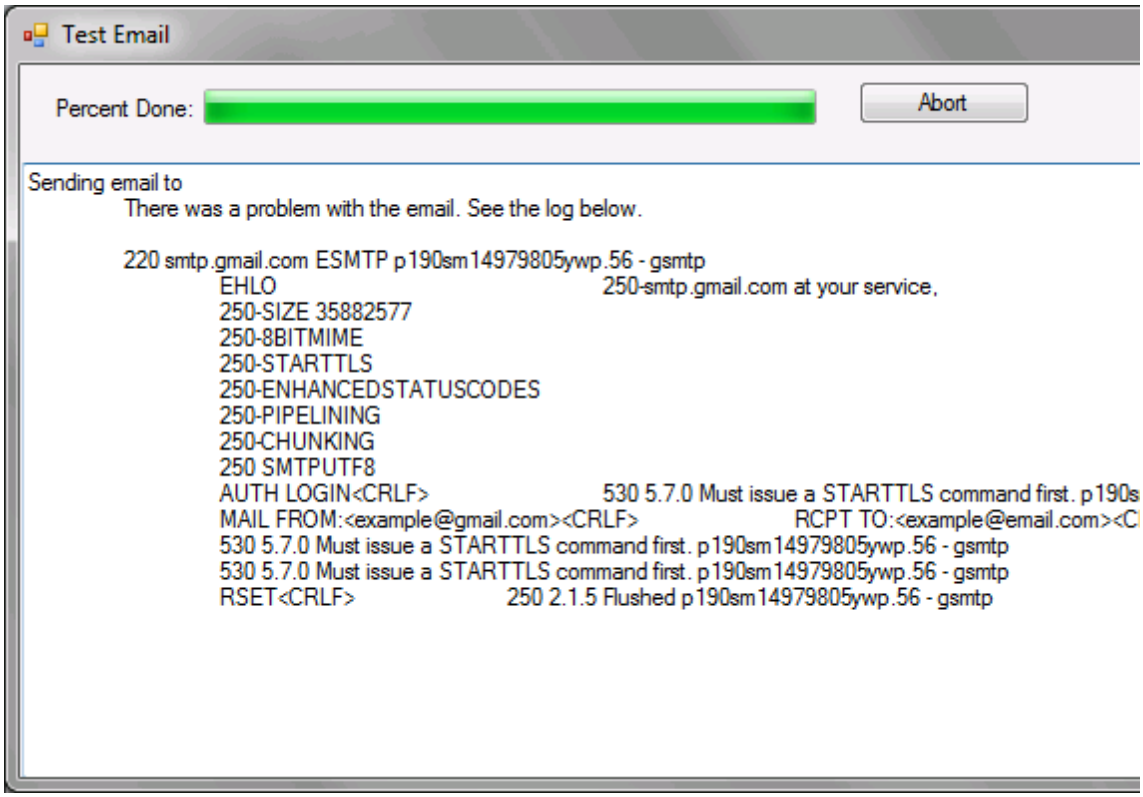
Troubleshooting Email Settings

If you have problems with setting up the email server, please contact your administrator. He/ She should know values to specify and how to test the settings.

Below is an example of what happens when the email server does not respond.

After a time out, you get a failure notice

After acknowledging the failure, you get a more detailed error message in the process result screen.



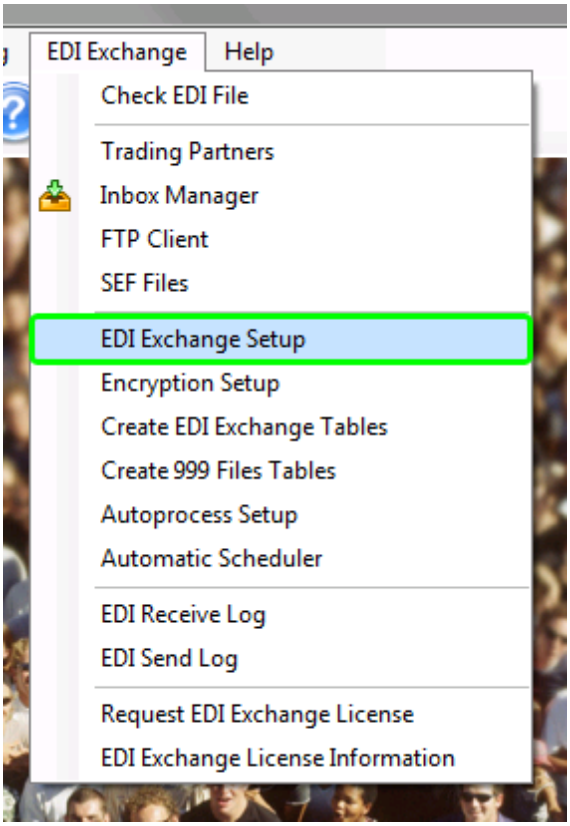
The process result screen with a detailed error message

9.3.2 Setting up Incoming and Outgoing Files Options

To check if your files are HIPAA-compliant, EDI Exchange can run a compliance check on outgoing EDI files. For incoming files, you can specify an acceptable error level. These settings are especially important with new trading partner relationships or with new processes since it always takes a while until an EDI process runs without issues and problems.

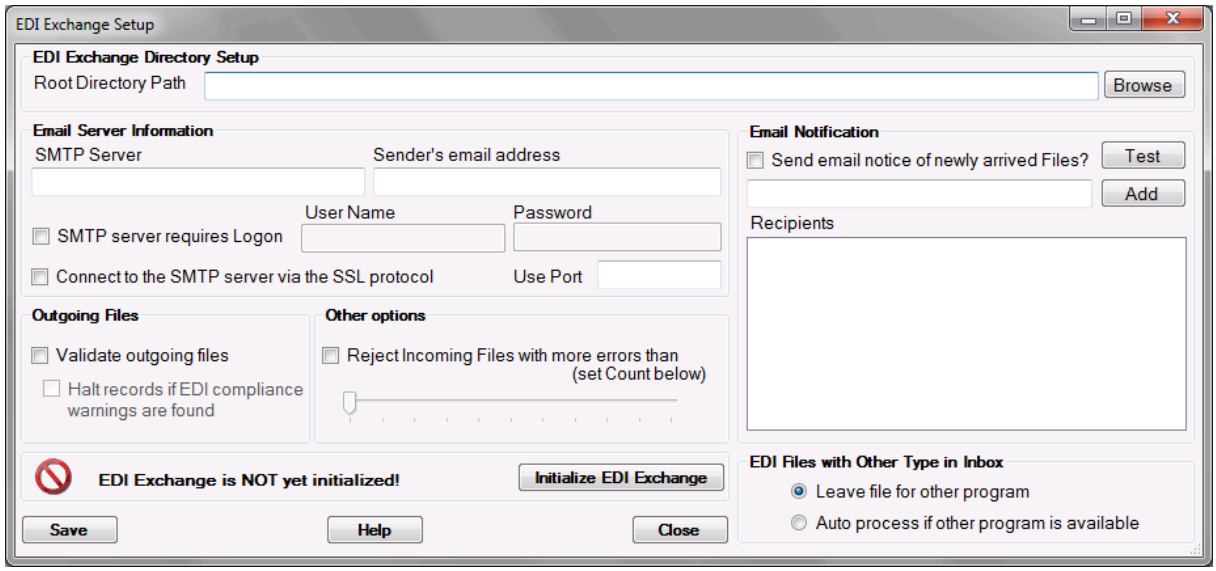
Follow the instructions below.

1. Select "EDI Exchange Setup" under the "EDI Exchange" menu item.



The "EDI Exchange Setup" menu item

2. The following window will appear.

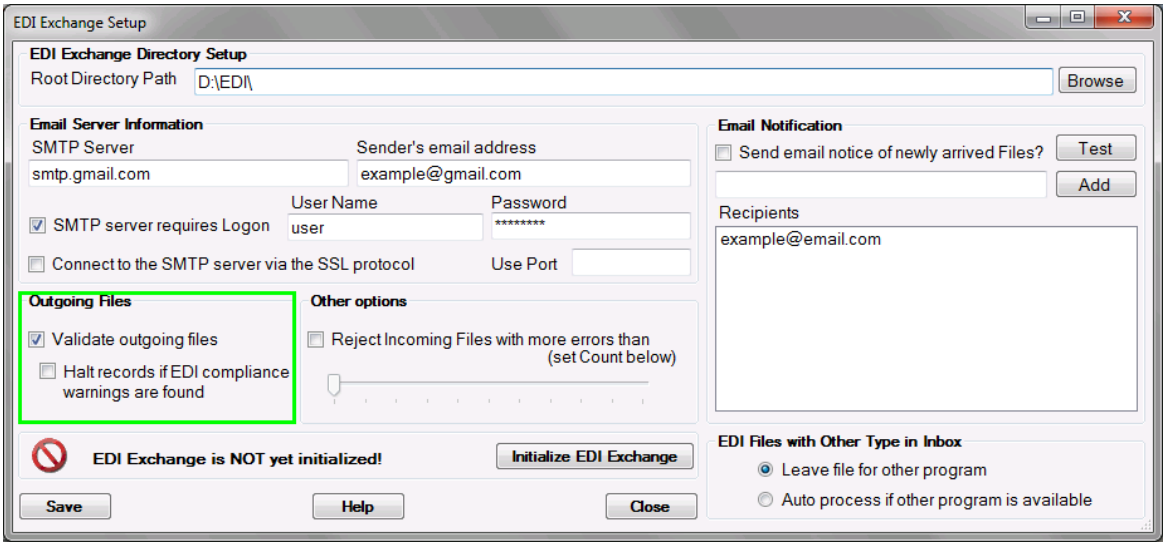


The "EDI Exchange Setup" window

3. Specify the following outgoing files options:

Outgoing Files

- **Validate outgoing files** — Select this checkbox to validate if the outgoing files are HIPAA-compliant.
    - **Halt records if EDI compliance warnings are found** — Select this checkbox to suppress the sending of files with warnings or errors.

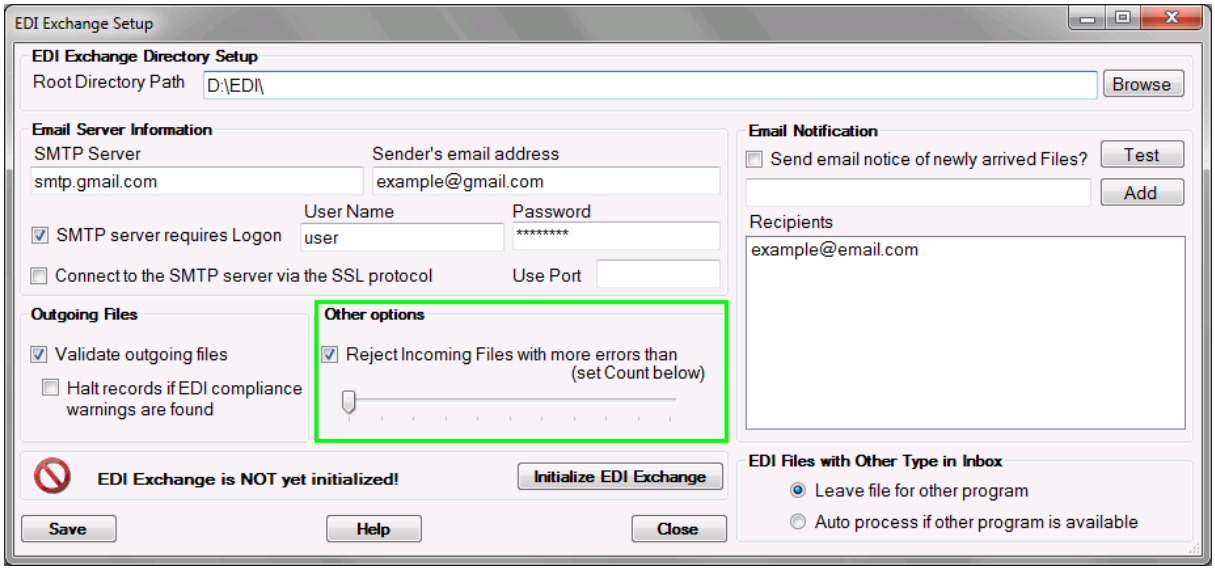


Validating outgoing files

4. Specify the following incoming files options:

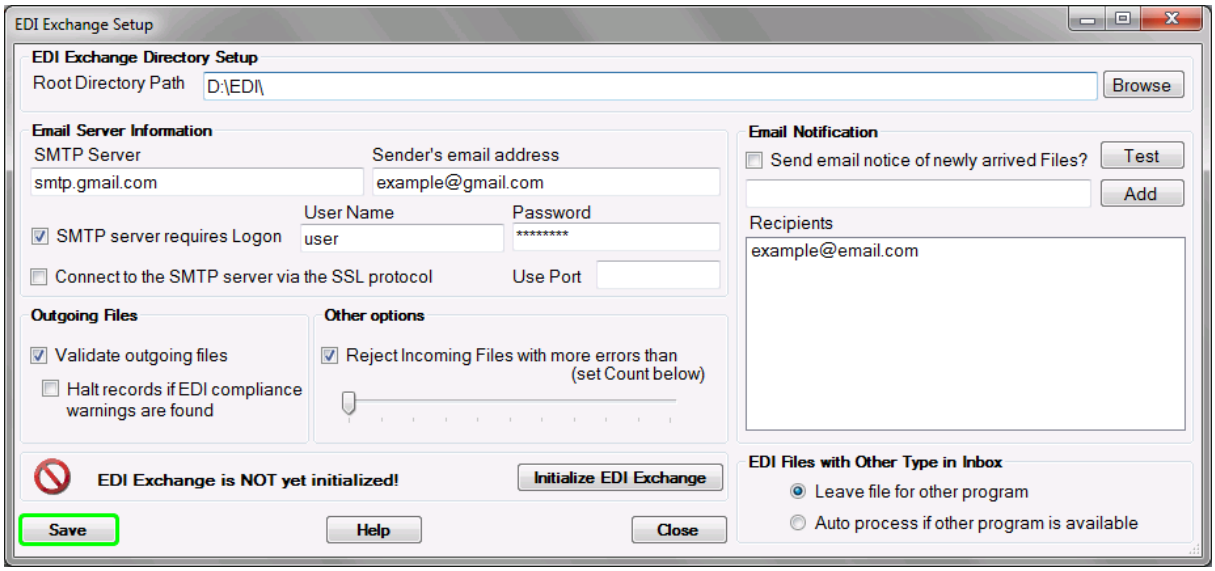
Other Options

- **Reject incoming files with more errors than (set count below)** — If checked, the incoming files with more errors than defined will not be placed into the "Inbox" folder.



The "Reject incoming files with more errors than" option

5. Click on "Save."



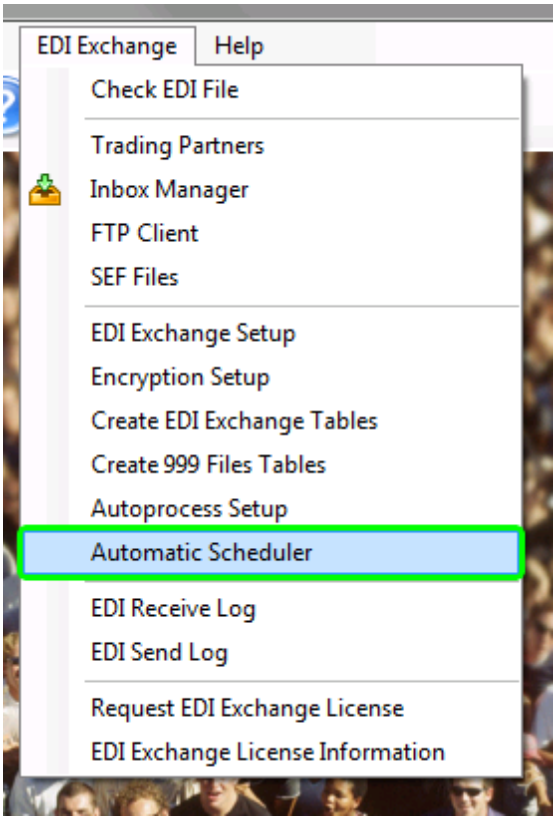
9.3.3 Running the Application via Scheduler

EDI Exchange integrates with the Windows Scheduler to allow the automation of the EDI file exchange process. You can set up EDI Exchange to go out to the trading partner's FTP server, download files, decrypt and compliance check them and further process them with the appropriate HIPAAsuite application, for example load claims into a SQL

database.

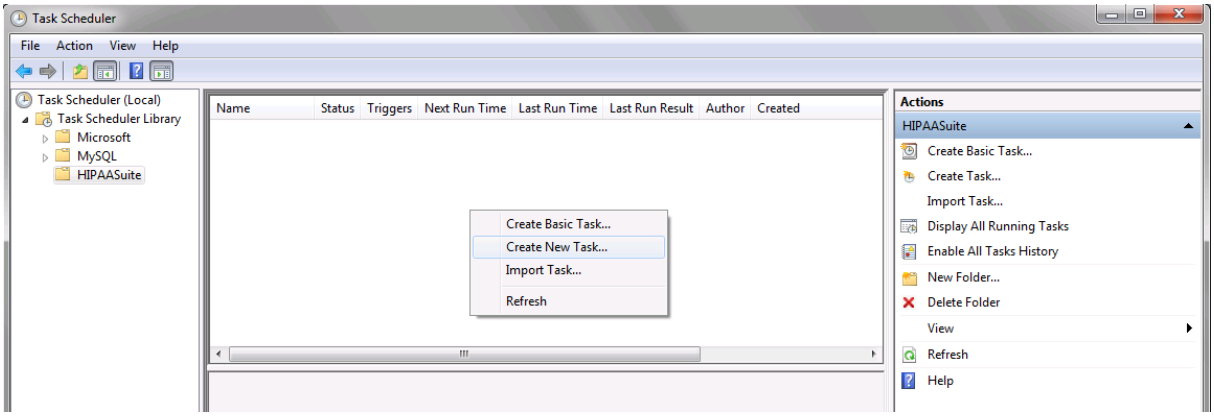
Follow the instructions below to schedule the EDI files exchange process.

1. Select "Automatic Scheduler" under the "EDI Exchange" menu.



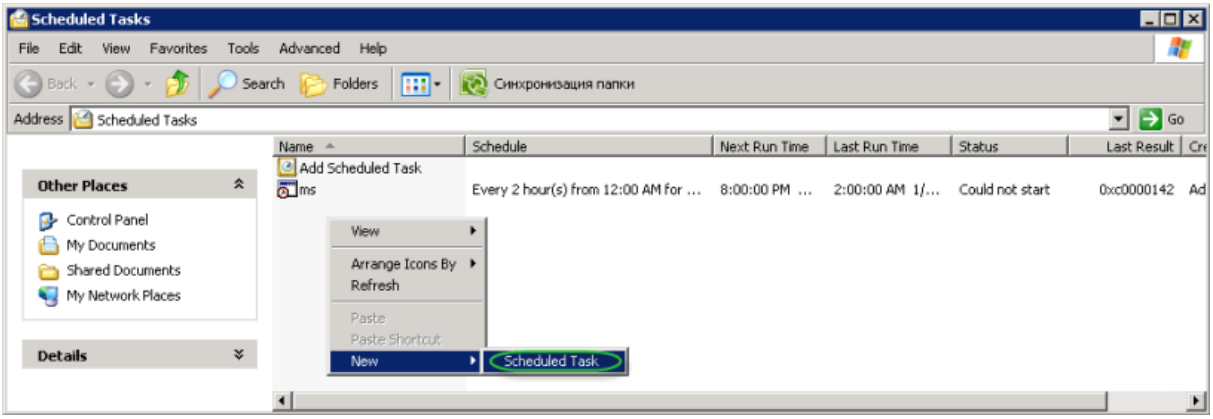
The "Automatic Scheduler" menu item

2. In the opened window, right click and choose the "Scheduled Task" menu item.



Task Scheduler in Windows Vista onwards.

In Windows XP, the Scheduled tasks directory looks like this:



The "Scheduled Task" menu item in Windows XP.

See "Running the Application via Scheduler" in the help of the host HIPAA application for detailed instructions on how to schedule a task.

9.3.4 Using the Command Line Arguments (CLI)

The only EDI Exchange specific command line argument is "Auto"

The Auto processing options are defined in another screen and, with the command line argument "Auto," they will be exercised. Make sure that you have configured them according to your needs.

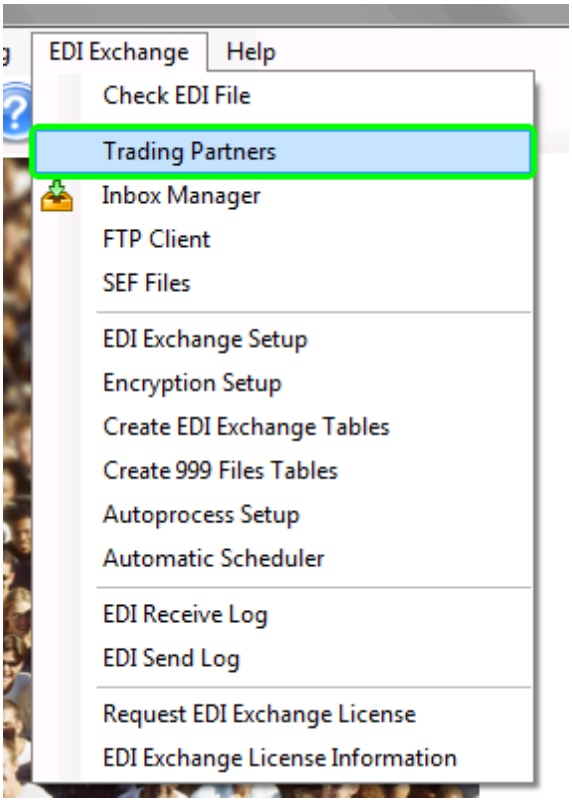
9.4 Working with Trading Partners

9.4.1 Setting up Trading Partners

With EDI Exchange you can keep track of your trading partners. You can set up their identifiers to send them EDI files or 999 acknowledgment, send email notifications and compliance check results, encryption keys and file transport mechanisms.

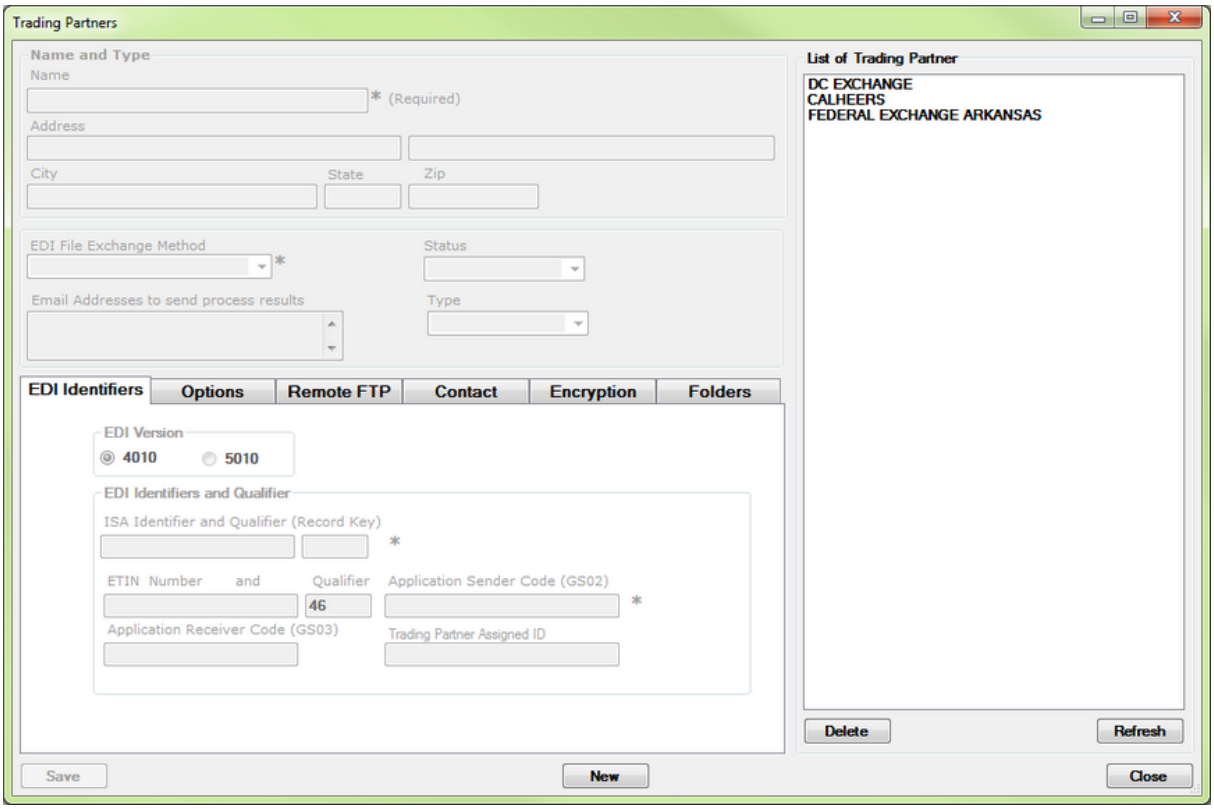
Once you have created the trading partner table (see Creating Database Tables) and initialized EDI Exchange (see Initializing EDI Exchange), you can set up the relationships with your trading partner. Follow the instructions below.

1. Select "Trading Partners" under the "EDI Exchange" menu.



The "Trading Partners" menu item

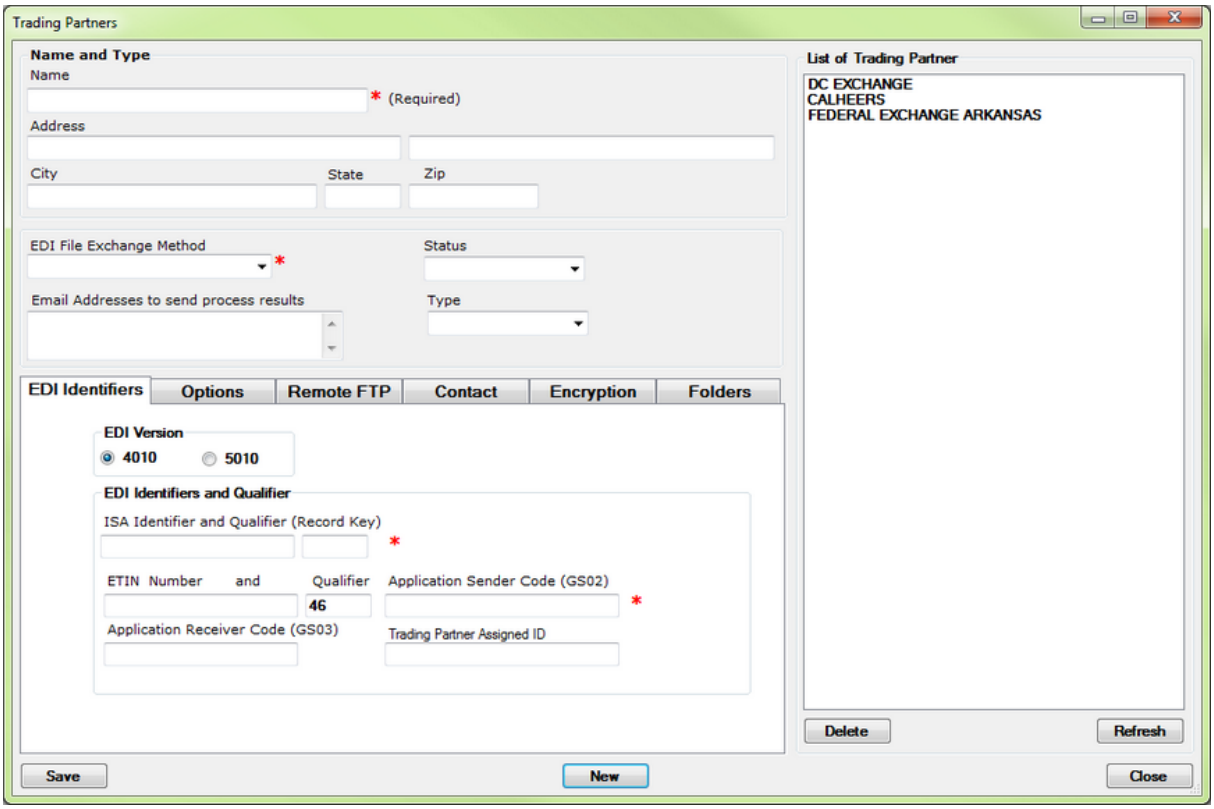
2. The following screen will appear.



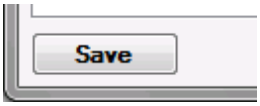
The "Trading Partners" window

3. Click the "New" button to start entering the trading partner information.

4. Define the necessary options. They are described further.



5. Click on "Save."

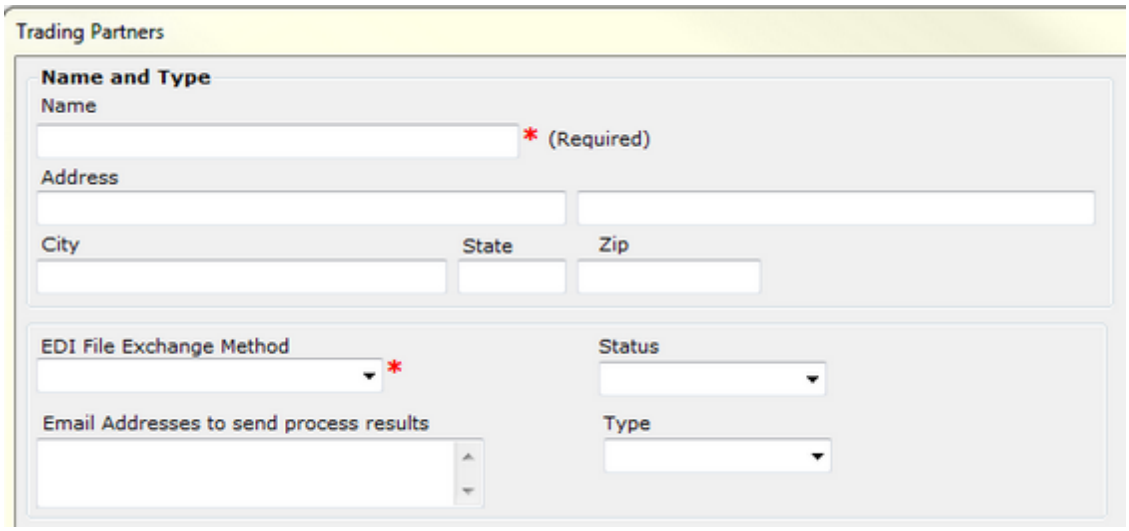


The "Save" button

6. The newly added Trading Partner's name will appear in the right pane.

Trading Partner Options

The company information of a trading partner can be specified on the top of the form.



Top area of the "Trading Partners" window

Name and Type

- **Name** — Trading partner's company name. Required field.
- **Address** — Trading partner's company address.
- **City**
- **State**
- **Zip**
- **Status** — Trading partner's status. Choose one of the available options:
  - **Inactive** — No upload into a database system through ODBC will be done.
  - **Test Only** — All outgoing EDI messages will be stamped with "Test" (ISA_15). Records will only be exported to the test environment.
  - **Approved** — All outgoing EDI messages will be stamped with "Production" (ISA_15). Records will be exported to the Live system with ODBC.
- **Type** — There are five types of trading partners, select the necessary one:
  - **Providers** — Hospitals, doctors or other health care providers.
  - **VANs** — Value Added Networks like clearing houses or EDI Networks.
  - **Service bureaus** — Third party entities such as repricing organizations.
  - **Sponsors** — Entities that sponsor the benefits of subscribers such as MedicAid, government agencies or large employers.

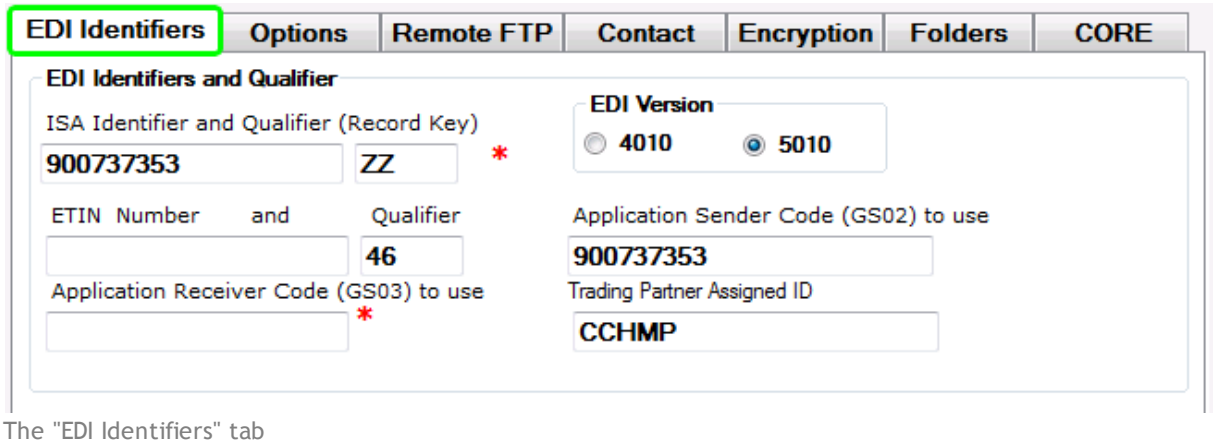
- **Payers** — Entities that pay for health care benefits such as health insurers.

The next block on the form lists the communication methods and preferences.

- **EDI File Exchange Method** — Obligatory setting. HIPAAsuite supports three communication methods. Choose a preferred mode of sending EDI communications to the trading partner:
  - **FTP** — Allows you to transmit files actively to the Trading Partner or his Clearinghouse.
  - **Outbox** — All files for Trading Partner are stored locally. The Trading Partner is responsible for picking up files in his special directory of the local FTP or HTTP server.
  - **SOAP** - Allows you to transmit files to the Trading Partner or his Clearinghouse using SOAP 1.2 (CORE) by default.
    - o **SOAP Version** - Defaults to CAQH CORE "SOAP 1.2". "SOAP 1.1" is also provided as a compatibility option for Trading Partners that are not yet CORE-Certified but use SOAP services.
  - **MIME** - Allows you to transmit files to the Trading Partner or his Clearinghouse using MIME (CORE). This is one of two CORE options.
- **Email Addresses** — Enter the email address(es) into the text field.

EDI Identifiers Tab

This tab relates to the EDI identifiers and EDI Version.



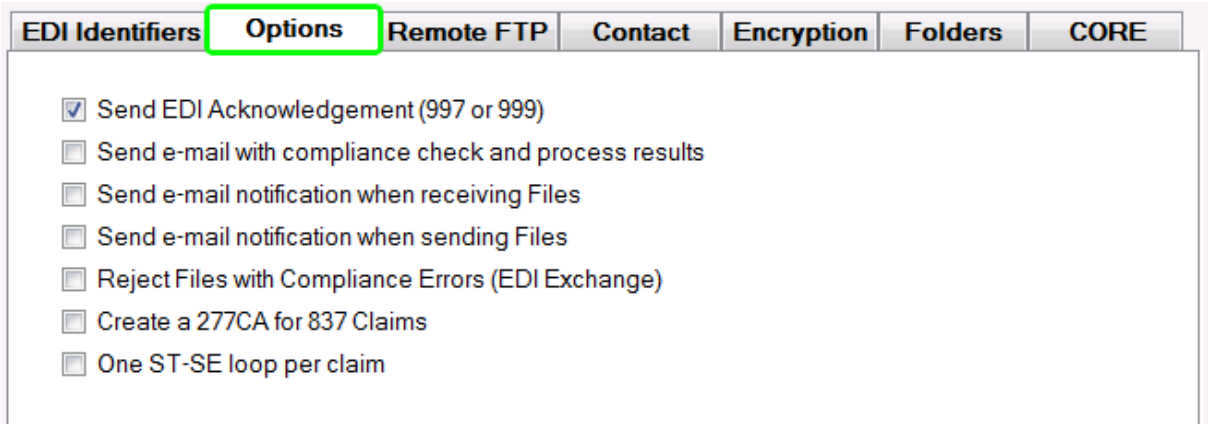
The "EDI Identifiers" tab

- **EDI Version** — There are two standards for HIPAA:

- 4010 — This standard was introduced in the original transaction from 2003 to 2011.
- 5010 — From 2012 on all HIPAA transactions must be conducted in the 5010 version.

- **EDI Identifiers and Qualifier**
  - **ISA Identifier and Qualifier (Record Key)** — The ISA Identifier and Qualifier are the unique key to the trading partner database file. The ISA identifier can be up to 15 bytes long, the qualifier has to be 2 bytes. Approved qualifiers are:
    - **01** — Duns (Dun and Bradstreet)
    - **14** — Duns Plus Suffix
    - **20** — Health Industry Number (HIN)
    - **27** — Carrier Identification Number as assigned by HCFA
    - **28** — Fiscal Intermediary Identification Number as assigned by HCFA
    - **29** — Medicare Provider and Supplier Identification Number as assigned by HCFA
    - **30** — U.S. Federal Tax Identification Number
    - **33** — National Association of Insurance Commissioners Company Code (NAIC)
    - **ZZ** — Mutually Defined. Many organizations use the ZZ qualifier with their name as the ID, for example ZZ and HIPAASUITE.
  - **ETIN number** — The Electronic Transmitter Identification Number established by a Trading Partner Agreement. This number occurs only in the 837 transactions. Often, the ETIN is same as the ISA ID.
  - **Application Receiver Code (GS_02)** — A code identifying a part that sends a transmission or the specific application within the sender's organization. Codes are agreed by Trading Partners. Again, usually this code is same as the ISA ID. This code is placed in the GS_02 element in the Functional Group Header (GS). Some Trading Partners want to send a specific code in GS_03, the application receiver code. You can enter it into the corresponding field. Most of the time it is not necessary.
  - **Assigned ID** - Some trading partners, like health insurance exchanges will give a plan an ID that is different from the ISA identifier defined in the Company Setup screen of the application. Especially in the creation of filenames is this Assigned ID important.

Options Tab



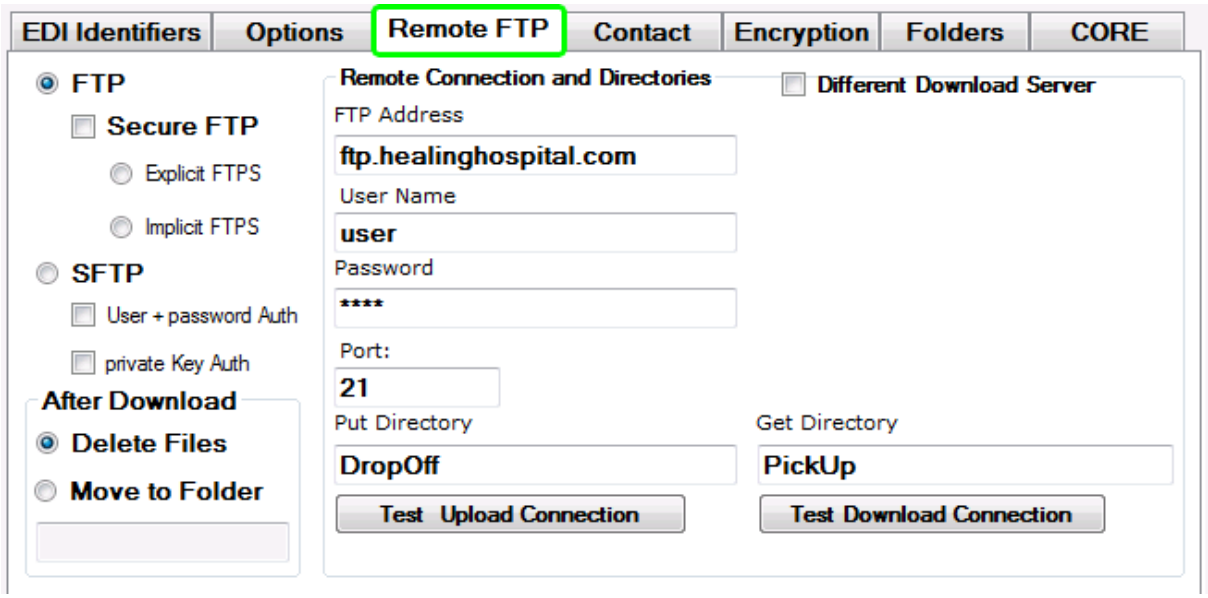
The "Options" Tab

You can choose one of the following options:

- **Send EDI Acknowledgment (997 or 999)** — This check-box allows sending Functional Acknowledgment transactions to the Trading Partner.
- **Send e-mail with compliance check and process results** — This option allows sending the compliance check results back to your contact at the Trading Partner via email. No PMI will be transmitted. Adding an email address is important, even when the Communication method is not "Email."
- **Send e-mail notification when receiving files** — This option allows sending an acknowledgment email of EDI files. This option is not necessary when you choose 997 or 999 acknowledgments.
- **Send e-mail notification when sending files** — This option allows sending a file to the Trading Partner notifying them that a file has been created for them.
- **Reject Files with Compliance Errors -** This option will reject files that have compliance warnings and move them into the suspended files directory. It also determines whether the TA1 and 999 indicate acceptance or the 999 lists all the errors and warning.
- **Create a 277CA for 837 claims** — This option only applies to 837 Claims. Checking this option will produce a 277CA Claims Acknowledgment report for received 837 Claim files.
- **One ST-SE loop per claim** - This option separates all claims into individual transactions enclosed by their own ST and SE segments.

Remote FTP Tab

If your trading partner has an FTP Server, then you can set up here the connection information. Read more in Using Built-in FTP Client.



The "Remote FTP" tab

The file transfer protocol (FTP) is one of the first internet protocols and goes back to the 1960's. Transporting electronic files was one of the great achievements of the internet. During the last 50 years a lot of improvements to this protocol have been made, mainly to increase the security of the transfer.

- **FTP** — For security reasons, EDI Exchange supports secure FTP or FTPs.
  - **Explicit FTPS Connection** — The explicit method is a legacy compatible implementation where FTPS aware clients can invoke security with an FTPS aware server without breaking overall FTP functionality with non-FTPS aware clients. In explicit mode (also known as FTPS), an FTPS client must "explicitly request" security from an FTPS server and then step-up to a mutually agreed encryption method. If a client does not request security, the FTPS server can either allow the client to continue insecure or refuse/limit the connection.
  - **Implicit FTPS Connection** — The implicit method requires that all clients of the FTPS server be aware that SSL is to be used on the session, and thus is incompatible with non-FTPS-aware clients. Negotiation is not allowed with implicit FTPS configurations. A client is immediately expected to challenge the FTPS server with a TLS/SSL ClientHello message. If such a message is not received by the FTPS server, the server should drop the connection. In order to maintain compatibility with existing non-TLS/SSL aware FTP clients, implicit FTPS was expected to listen on the IANA Well Known Port 990/TCP for the FTPS control channel and 989/TCP for the FTPS data channel. This allowed

administrators to retain legacy compatible services on the original 21/TCP FTP control channel.

- **SFTP** — also known as FTP over SSH is deemed the most secure form of FTP and uses encryption certificates. There are 3 different ways to authenticate a SFTP connection,
  - With user name and password, just like a regular FTP connection,
  - User name and a certificate
  - User name, certificate and password

Remote Connection and Directories

You need the FTP address, the user name and password to establish the connection and the directory information where files are picked up and where dropped off. Fill in the following fields:

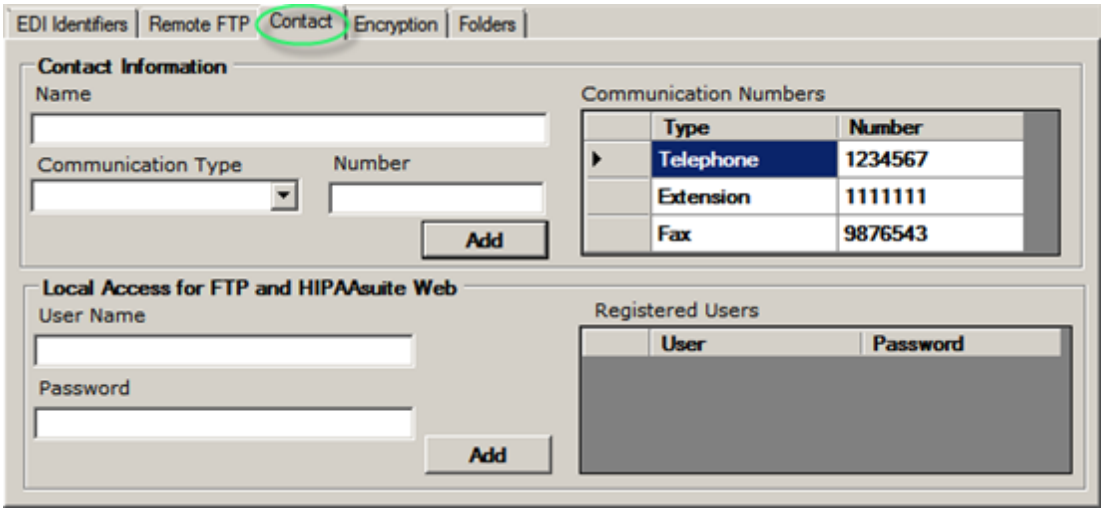
- **FTP Address -** This is usually the IP address of the server
- **User Name**
- **Password**
- **Put Directory -** This is the directory where you drop off files
- **Get Directory -** This is the directory where you download files from

It is possible that a trading partner has two FTP servers, one for 'put' and another one for 'get'. If so, check "Different Download Server" and additional fields will become visible so you can specify the those connection parameters.

After Download: You have two choices. Files on the server will be either deleted or moved to another folder of your choice .

Contact Tab

The Contact Tab stores contact information for your selected Trading Partner.



The "Contact" tab

Contact Information

Enter the name and the number into the corresponding fields and select the communication type from the drop-down list.

- **Contact Name**
- **Communication Numbers** — Valid Communication number qualifiers are:
  - **TE** — Stands for Telephone.
  - **FX** — Stands for Fax.
  - **EX** — Stands for Extension.
  - **EM** — Stands for email.

Click the "Add" button and the contact will appear in the "Communication Numbers" table.

> Note: The information that you fill in goes also into EDI files in the "PER" segment.

Local Access for FTP and HIPAAsuite Web

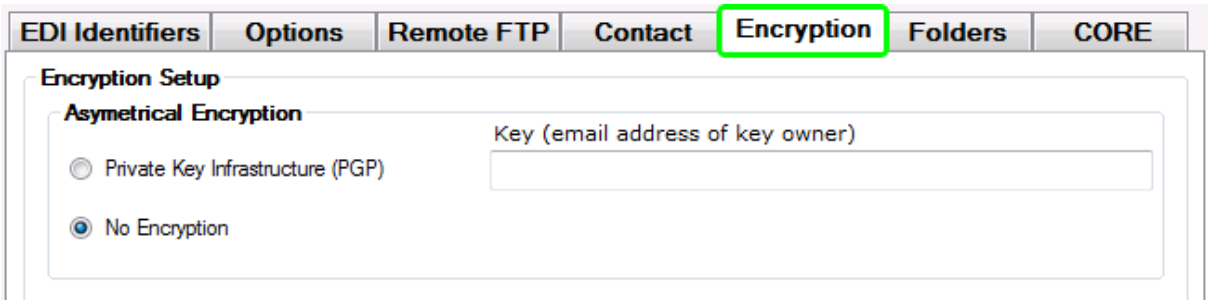
To register a user, enter the user name and the password into the corresponding fields and click the "Add" button. The user will appear in the "Registered Users" table.

- **User Name**
- **Password**
- **Registered Users**

Encryption Tab

EDI Exchange supports PKI encryption. Encryption keys are defined by the email address of the owner. Both supported products, PGP and GnuGP use this logic. Read more in Using Encryption.

You can set up the encryption parameters for a Trading Partner on the "Encryption" tab.



The "Encryption" tab

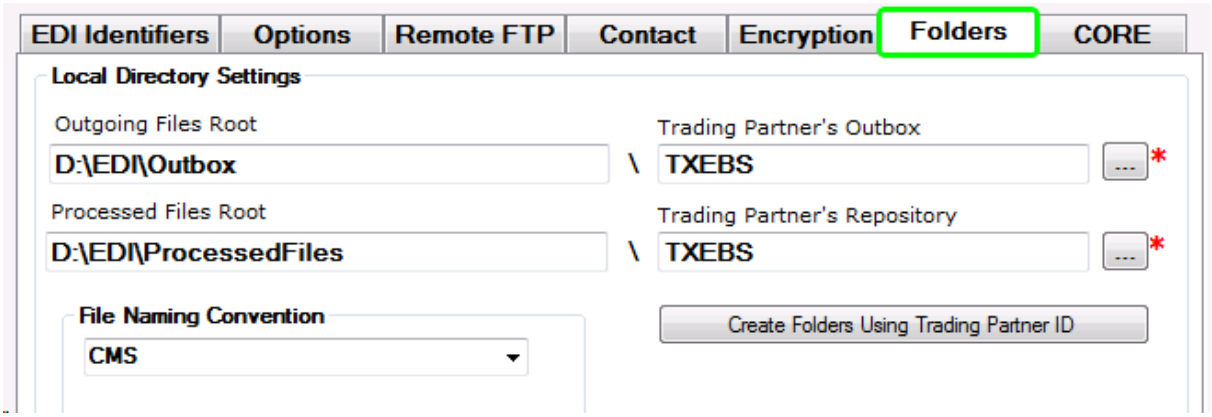
Encryption Setup

- **Asymmetrical Encryption**
  - **Private Key Infrastructure (PGP)**

    Key (email address of key owner)
  - **No Encryption**

Folders Tab

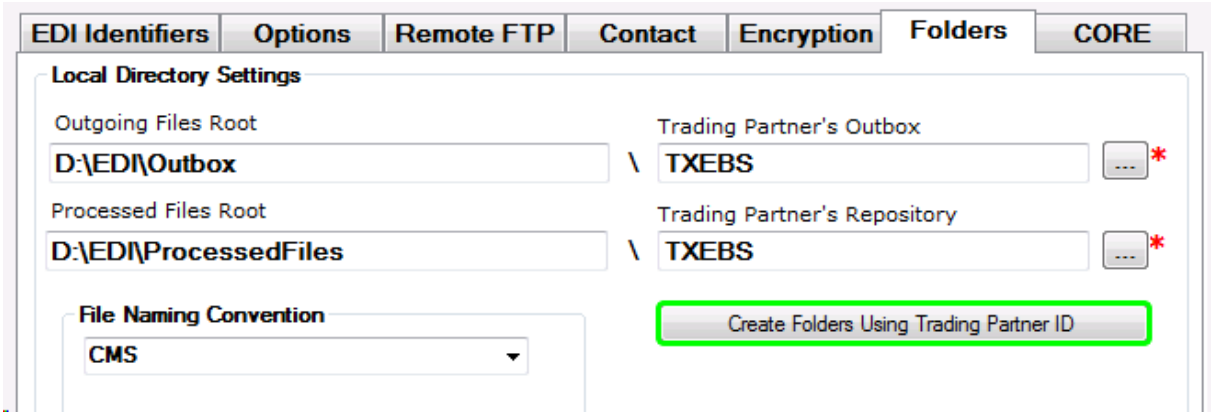
Within the HIPAAsuite Communications Directory, each Trading Partner has his own folder. This keeps files finely separated and in order. Here is where you can set this up. Read more in Defining Communications Directory.



The "Folders" tab

- **Outgoing Files Root** — This field has a pre-generated path. You can change this path by changing the EDI Root Directory.
- **Trading Partner's Outbox** — Mandatory setting. Click on the three-dots button to access the "Select Folder" window. There you choose an existing folder or create a new one.
- **Processed Files Root —** This field has a pre-generated path. You can change this path by changing the EDI Root Directory.
- **Trading Partner's Repository —** Mandatory setting. Click on the three-dots button to access the "Select Folder" window. There you choose an existing folder or create a new one.

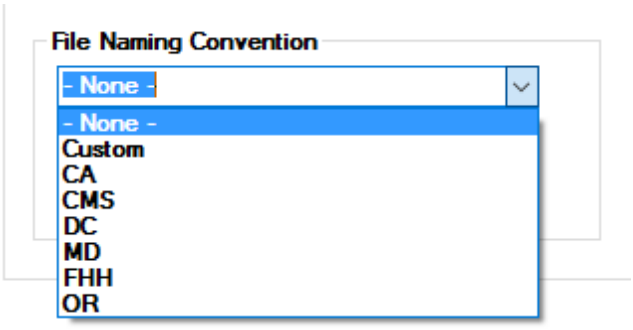
Once you have specified the directory settings, click on the "Create Folders Using Trading Partner ID."



The "Create Folders Using Trading Partner ID" button

- **File Naming Convention** - Health Insurance Exchanges (HIX) demand that a carrier adheres to more or less complex File naming conventions. Since these conventions are often really complicated we decided to hard code several schemes. California,

Maryland, DC and the CMS scheme are among those currently configured and we will add other schemes if needed.

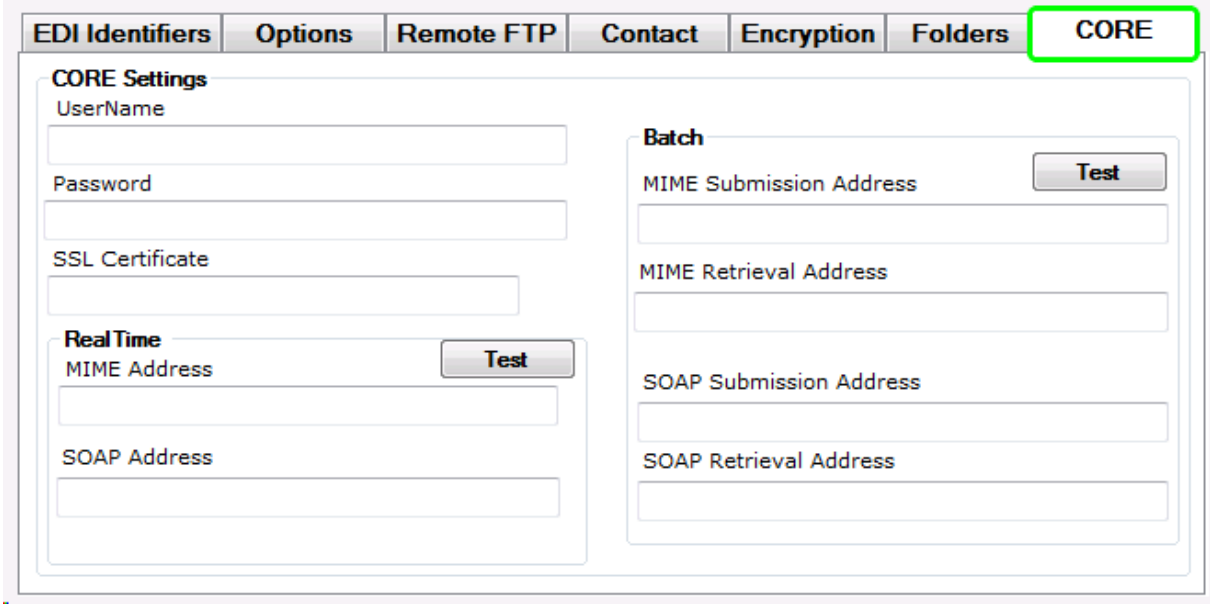


Filenaming dropdown menu options

The *Custom* File Naming Convention option requires some additional setup. This is covered in Custom File Naming Conventions.

CORE Tab

This tab stores settings for the use of CORE-Compliant SOAP- and MIME-enveloped transactions. When using a Requester or similar application, these settings apply to the information source. When using a Responder or similar application, these settings apply to the information requester/receiver. Soap 1.2 or 1.1 will use the same options.

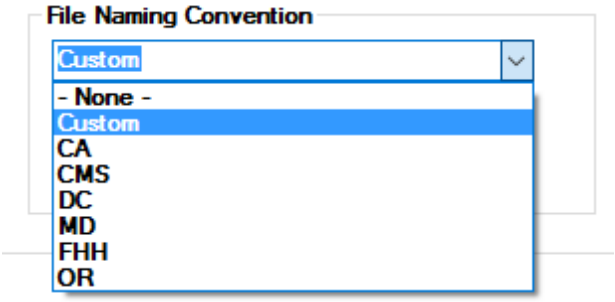


CORE settings tab

- **UserName** - UserName portion of the username authentication token. Used to verify a Trading Partner's Username token's Username or in your own Username token authenticate yourself to a Trading Partner's CORE-compliant servi e.
- **Password** - Password portion of the username authentication token. Used to verify a Trading Partner's Username token's Password or in your own Username token to authenticate yourself to a Trading Partner's CORE-compliant service.
- **SSL Certificate** - Instead of Username tokens, use an SSL certificate to verify a Trading Partner's identity or access a Trading Partner's CORE-compliant service. Not currently implemented.
- **RealTime**
  - **MIME Address** - Trading Partner's web address for MIME Real-Time transactions.
  - **SOAP Address** - Trading Pertner's web address for SOAP Real-Time transactions.
- **Batch**
  - **MIME Submission Address** - Trading Partner's web address for MIME Batch transactions.
  - **MIME Retrieval Address** - Some Trading Partners may use a different address to submit or retrieve batch transactions. Use this field for a retrieval-specific address.
  - **SOAP Submission Address** - Trading Partner's web address for SOAP Batch transactions.
  - **SOAP Retrieval Address** - Some Trading Partners may use a different address to submit or retrieve batch transactions. Use this field for a retrieval-specific address.

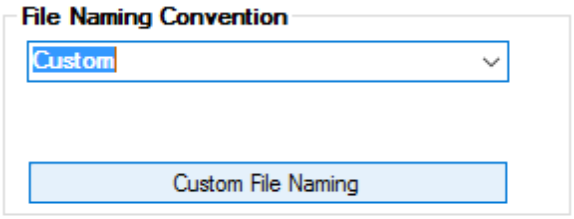
9.4.2 Custom File Naming Conventions

Health Insurance Exchanges (HIX) demand that a carrier adheres to File naming conventions. These file naming conventions enable a reader to quickly determine the date, time, sender, recipient, etc. of a particular file among other files without the need to open them individually. The custom File Naming Convention option enables you to create a file naming convention scheme tailored to your (or your trading partner's) requirements.



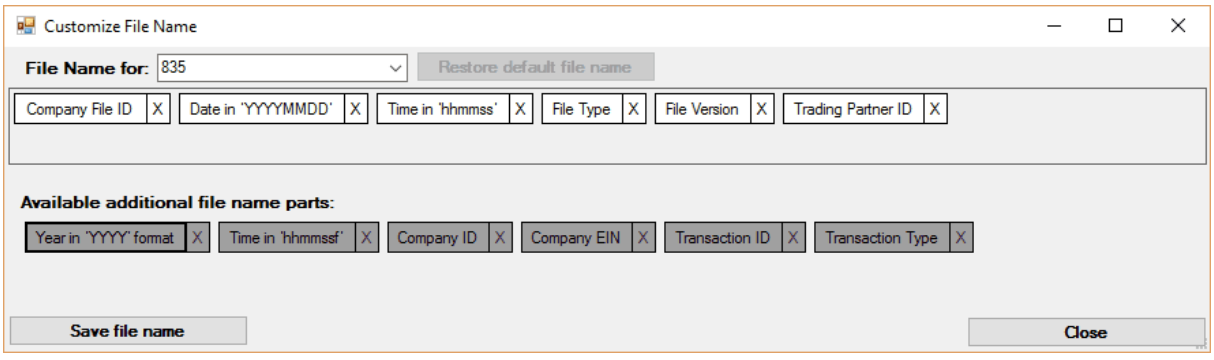
Custom File Naming Convention option highlighted

Selecting the Custom option in the File Naming Convention dropdown menu option and clicking the *Custom File Naming* button below it:



Custom File Naming button enabled

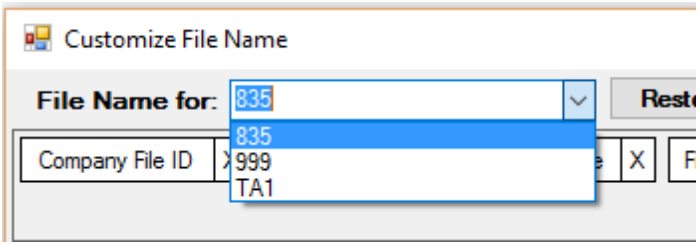
will bring up the screen pictured below. This screen is used to create file naming conventions for a particular trading partner. These examples will use the 835 file type as an example, but all file types the HIPAASuite product represents (as well as TA1s and 999s) can have their own file naming convention applied to each trading partner. The following picture shows the file name customization screen with the default building blocks for an 835 EDI file.



File Naming Customization screen with default custom file naming convention

Filetype

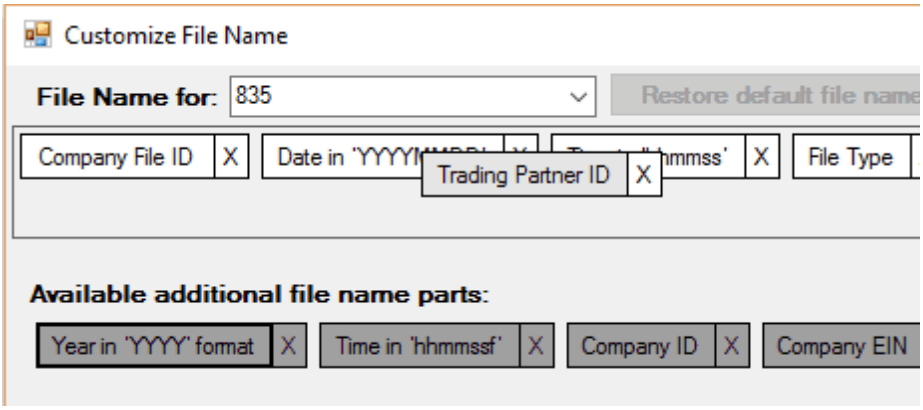
Here we can create a custom file naming convention for a specific file type. The file types available will depend on the HIPAASuite product used to create the file naming convention. To change the file type, select it from the file type dropdown menu:



Changing the filetype

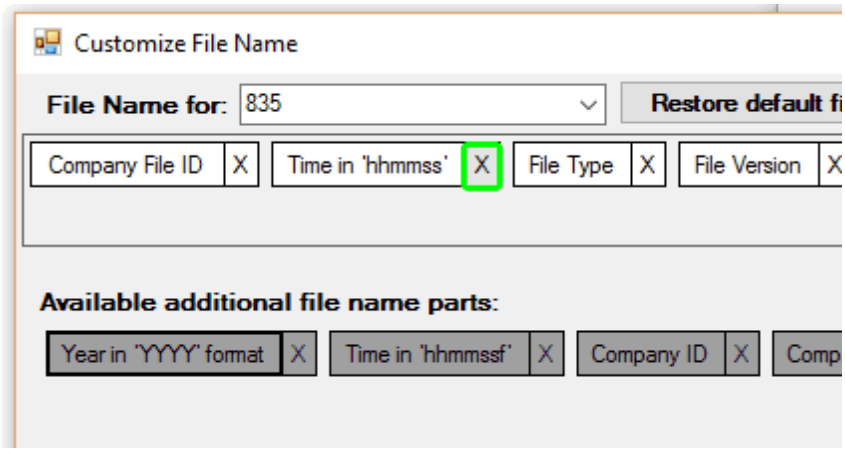
Creating the file naming convention

A coherent file naming convention can be created by clicking and dragging elements into order. Present elements can be reordered by clicking and dragging them into position:



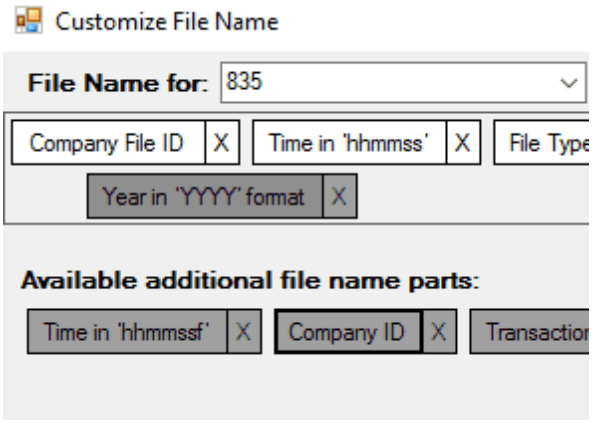
Click-dragging an element into position

Existing elements can be removed by clicking the *X* to the right of the element:



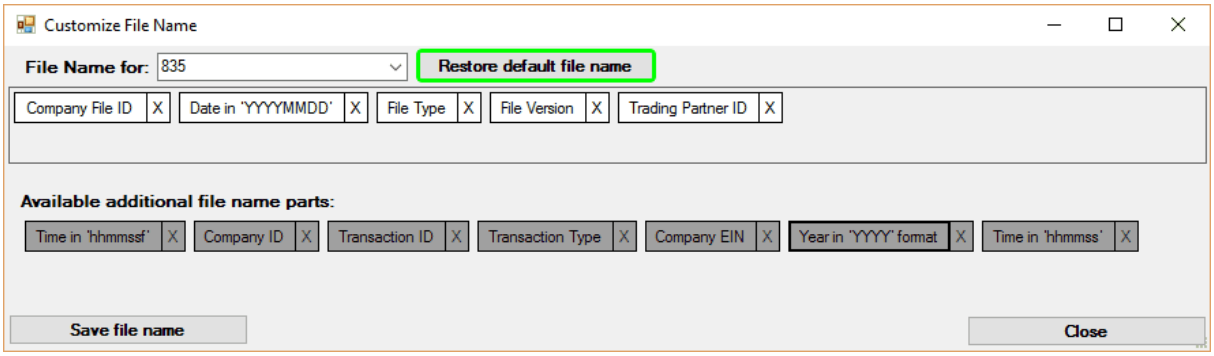
Deleting an element

The greyed-out elements towards the bottom of the screen can be added to the custom file naming convention by clicking and dragging them into place:



Adding a file name element

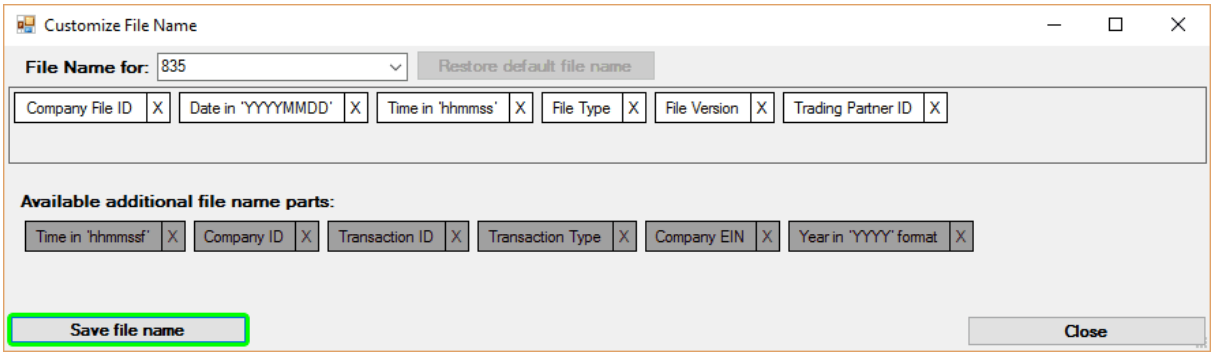
To discard the current changes and start over with the default file naming convention, click the *Restore default file name* button.



Restore default file name button

Saving or discarding

Finally, the custom file naming convention can be saved by clicking *Save file name* or discarded by clicking *Close*.



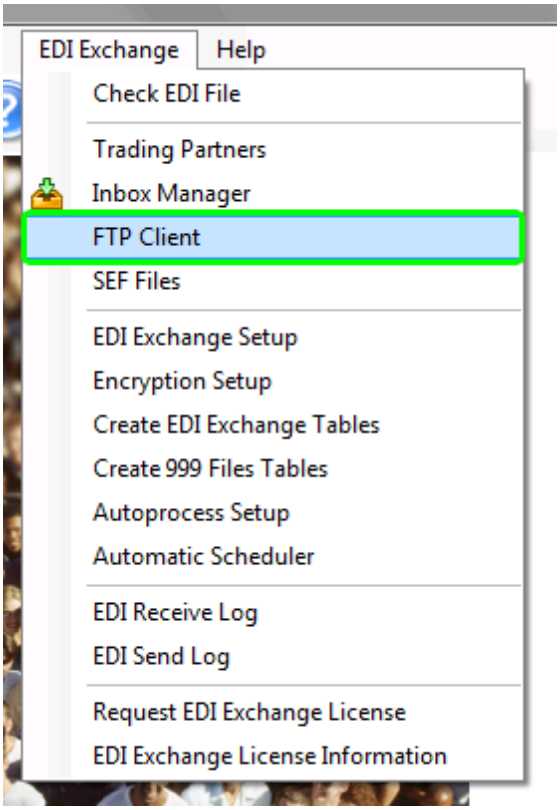
Save button on file name customization screen

9.4.3 Using Built-in FTP Client

EDI Exchange has a built-in FTP client. This utility allows you to drop-off and pick-up files from a trading partner that you have defined in the "Trading Partners" menu (see Setting up Trading Partners.)

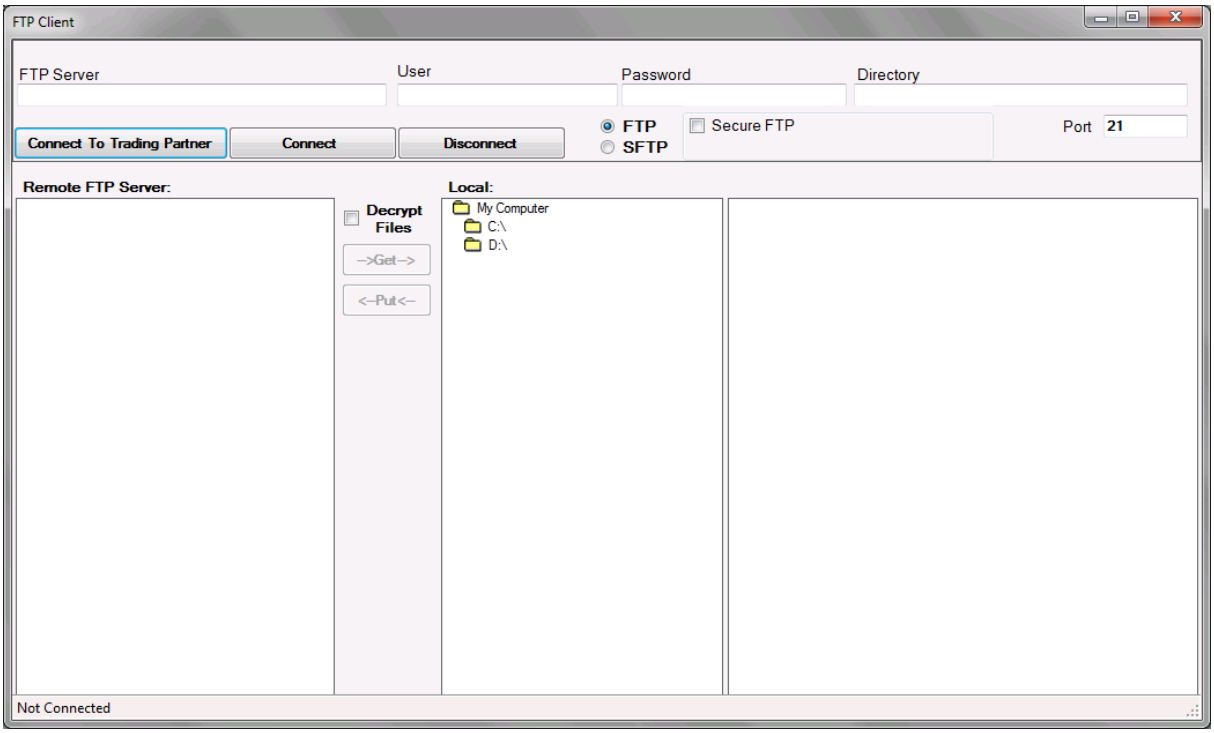
Follow the instructions below to exchange EDI files with your Trading Partner.

1. To access the FTP client, select "FTP Client" under the "EDI Exchange" menu item.



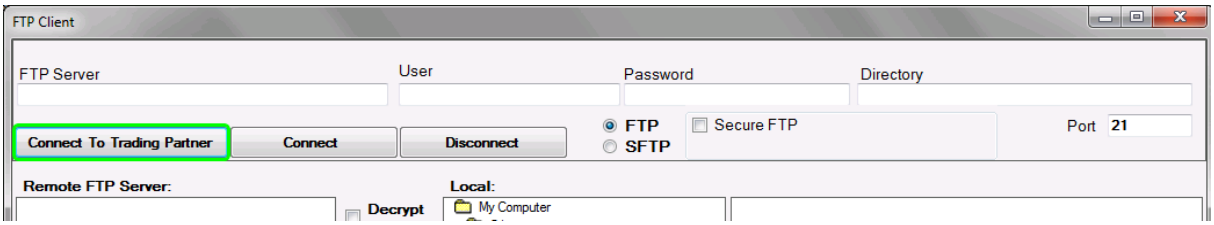
The "FTP Client" menu item

2. The following window will appear.



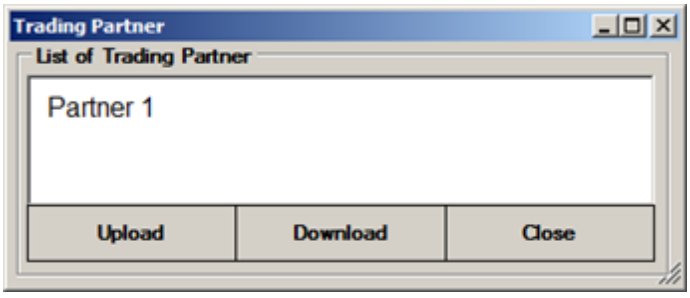
The built-in FTP client

3. Click the "Connect to Trading Partner" button on the FTP client window.



The "Connect to Trading Partner" button

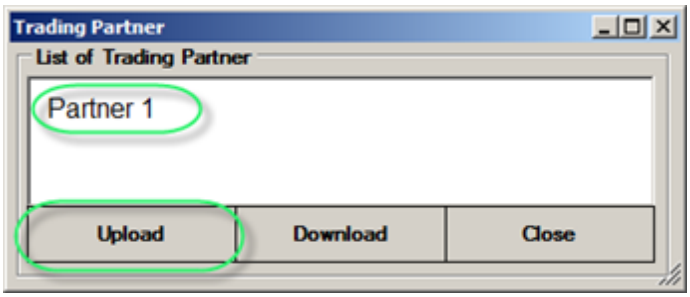
4. The following screen opens.



Selecting a Trading Partner for FTP transfer

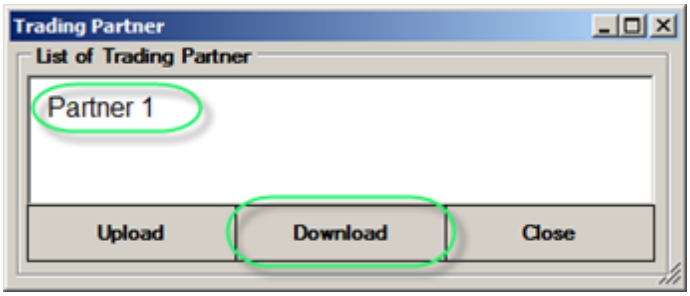
5. Highlight the trading partner that you want to connect to.

6. Click on the "Upload" button to connect to the "Put" directory that you set up in the trading partner screen.



The "Upload" button

Or click on the "Download" button to connect to the "Get" directory that you set up in the trading partner screen.



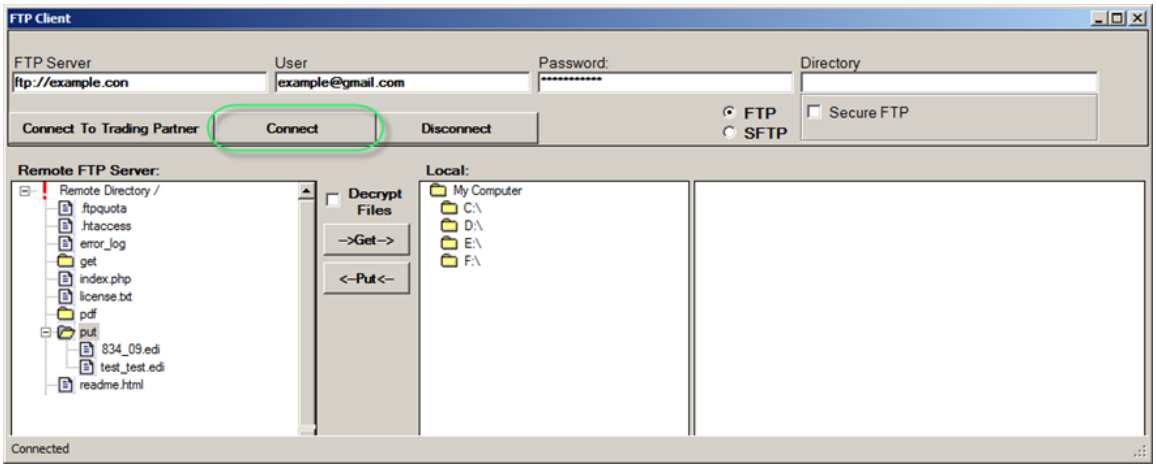
The "Download" button

5. Once you have chosen a trading partner, the following fields will contain values derived from the trading partner's properties. You can change them manually if you need.

- **FTP server** — IP Address or URL of the FTP server.
- **Username**
- **Password**
- **Directory** — If you leave this value blank, the FTP root directory will be opened.
- **Secure FTP** — If you enable this option, then you can select between implicit and explicit FTPs. See Setting up Trading Partners for an explanation of the two secure methods:
  - **Explicit FTPS Connection**
  - **Implicit FTPS Connection**

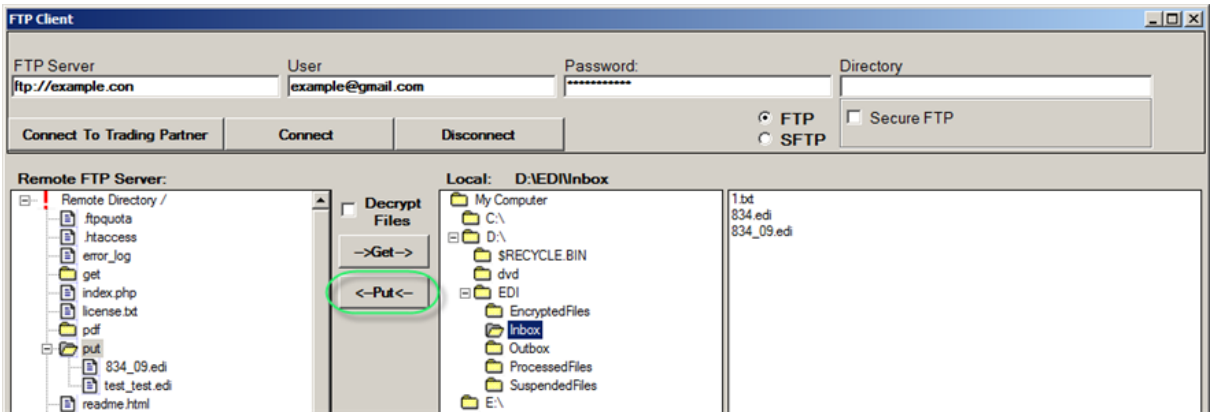
Note: You can also fill in the connection information manually. In this case, the entered credentials will not be saved once you close the FTP client window. Click on the "Connect" button to establish

connection to the FTP server.

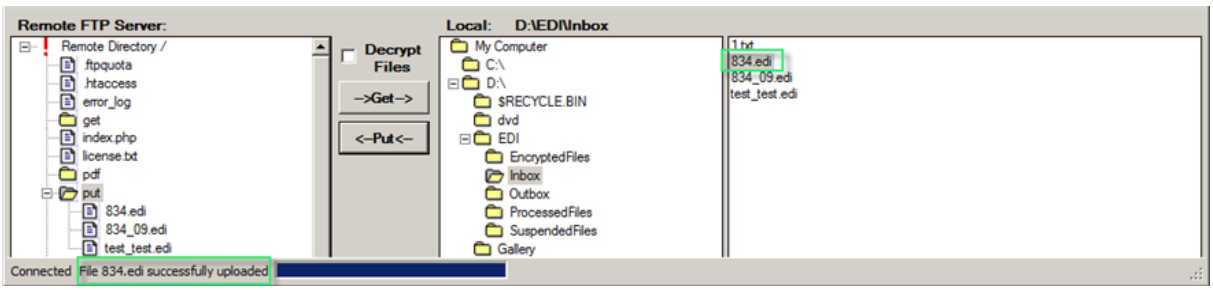


4. Once connected, the content of the folder on the server is displayed. On the right side, you can browse your local PC.

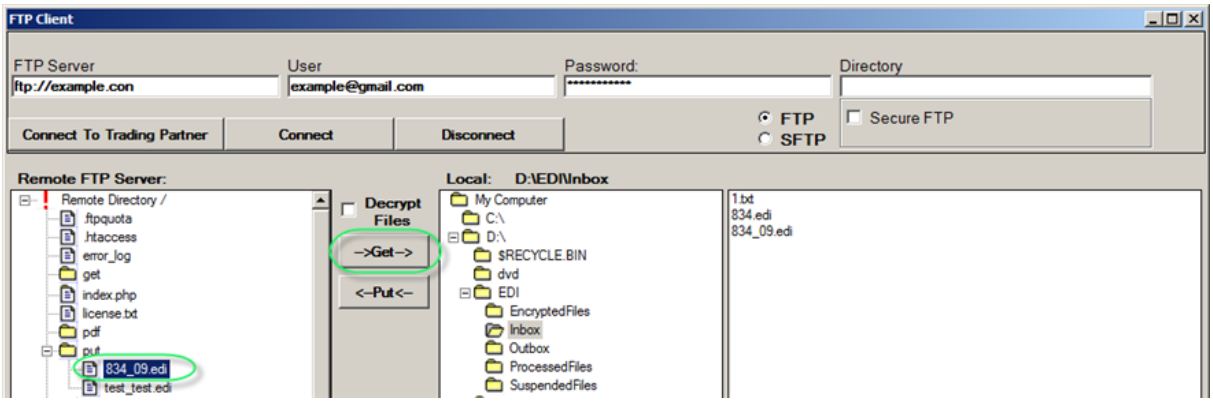
5. To upload a file to the server, select the file on your local PC and click on the "Put" button.



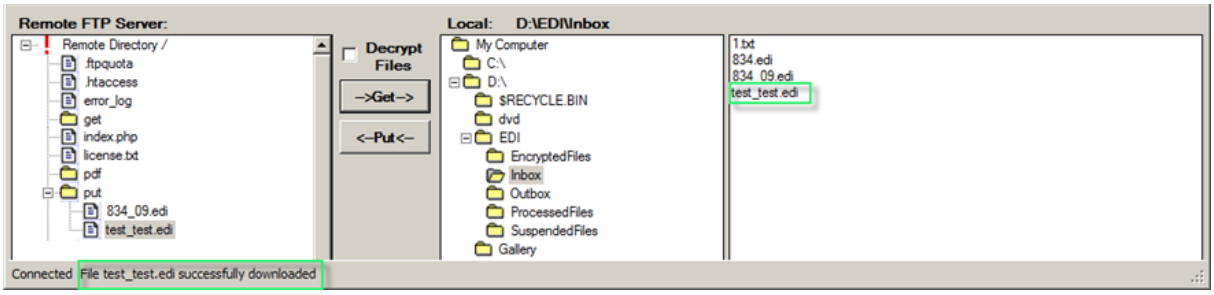
The file will appear in the remote folder. You will receive the "File <filename> successfully uploaded" message on the bottom status bar of the FTP client.



6. To download a file from the server, select a file in the left side, and then click on the "Get" button.

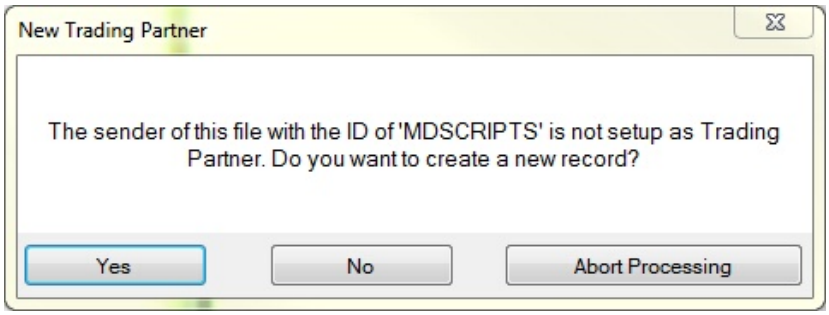


The file will appear in the local folder. You will receive the "File <filename> successfully downloaded" message on the bottom status bar of the FTP client.



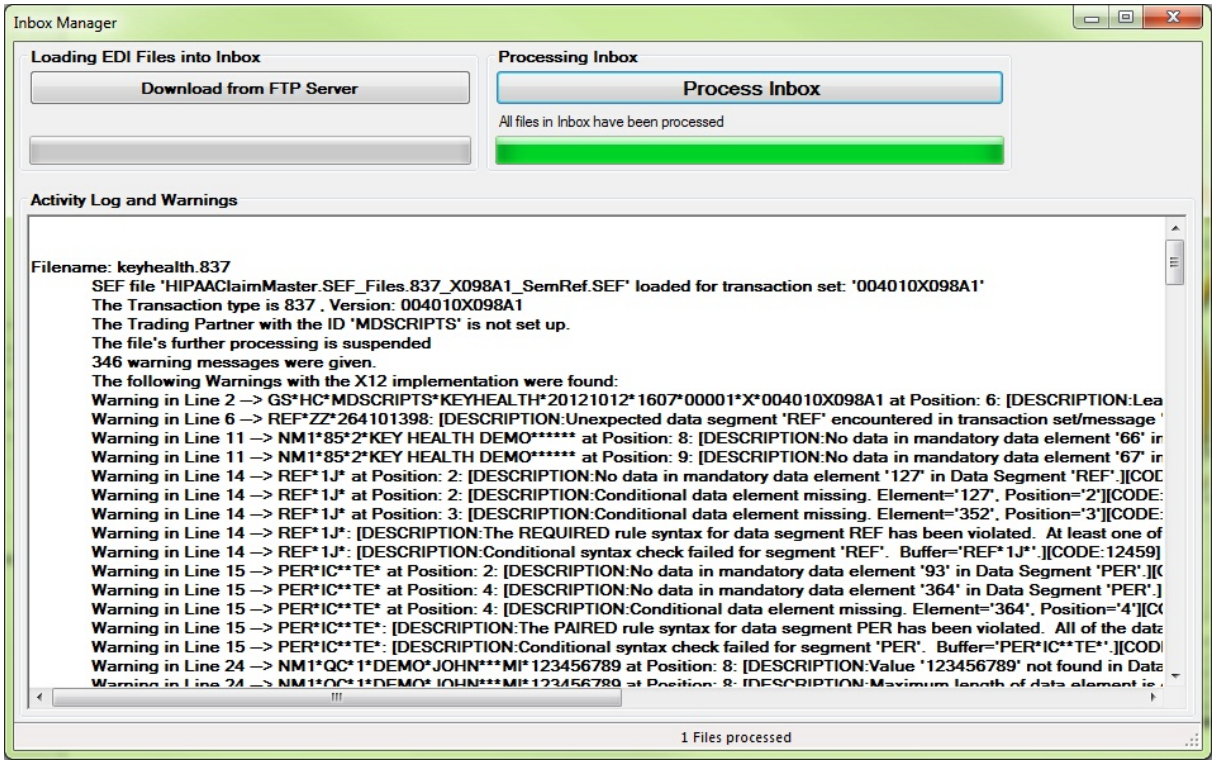
9.4.4 Creating a Trading Partner Automatically

When you process a file with EDI Exchange the sender's ID is compared to the trading partners on file. If the trading partner does not exist you have the opportunity to create a rudimentary new trading partner record. Now you have the choice to either create this new record, process the file without the trading partner record or to abort the operation.



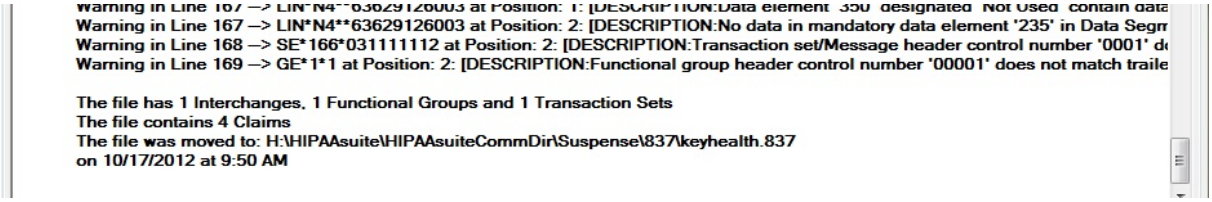
The "New Trading Partner" dialog box

If you abort the process, you still will get the EDI file analysis.



EDI compliance check results after further processing was aborted.

Files without a valid trading partner will be placed into the "suspended files" directory. The final action taken after the analysis is recorded at the end of the results.



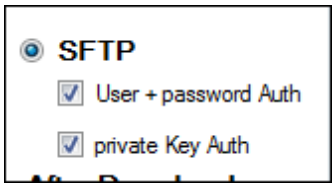
This file's processing was aborted. The file was moved to the suspended files folder

9.4.5 Certificate based authentication in SFTP

SFTP or FTP over secure shell as it is also known is deemed to be the most secure method of file transport. There are 3 methods of authentication in Sftp.

1. with a user name and password
2. with a user name and a private key cryptographic certificate and
3. with a user name, a certificate and a password

When you select SFTP as the FTP protocol, you will see two check boxes appear.



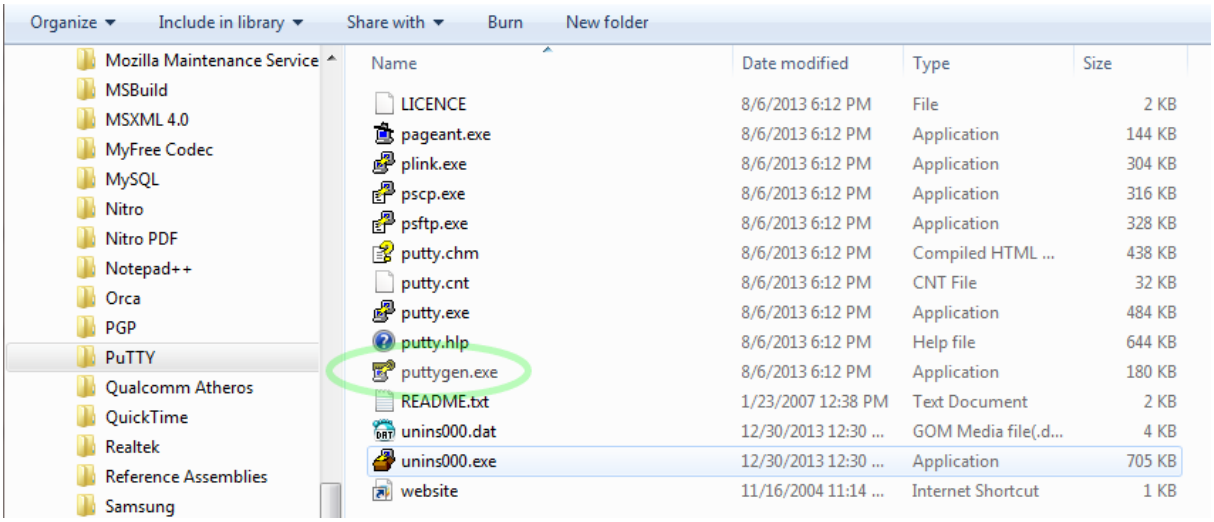
The sub choices when you select SFTP

Leaving both check boxes unchecked will result in the first option: Authentication with user name and password. You can also check just the user name and password with the same result.

In order to use the certificate based authentication you need to create and link to your own certificate. The certification module that HIPAAsuite employs uses a so called private key SSH2 certificate in pem format.

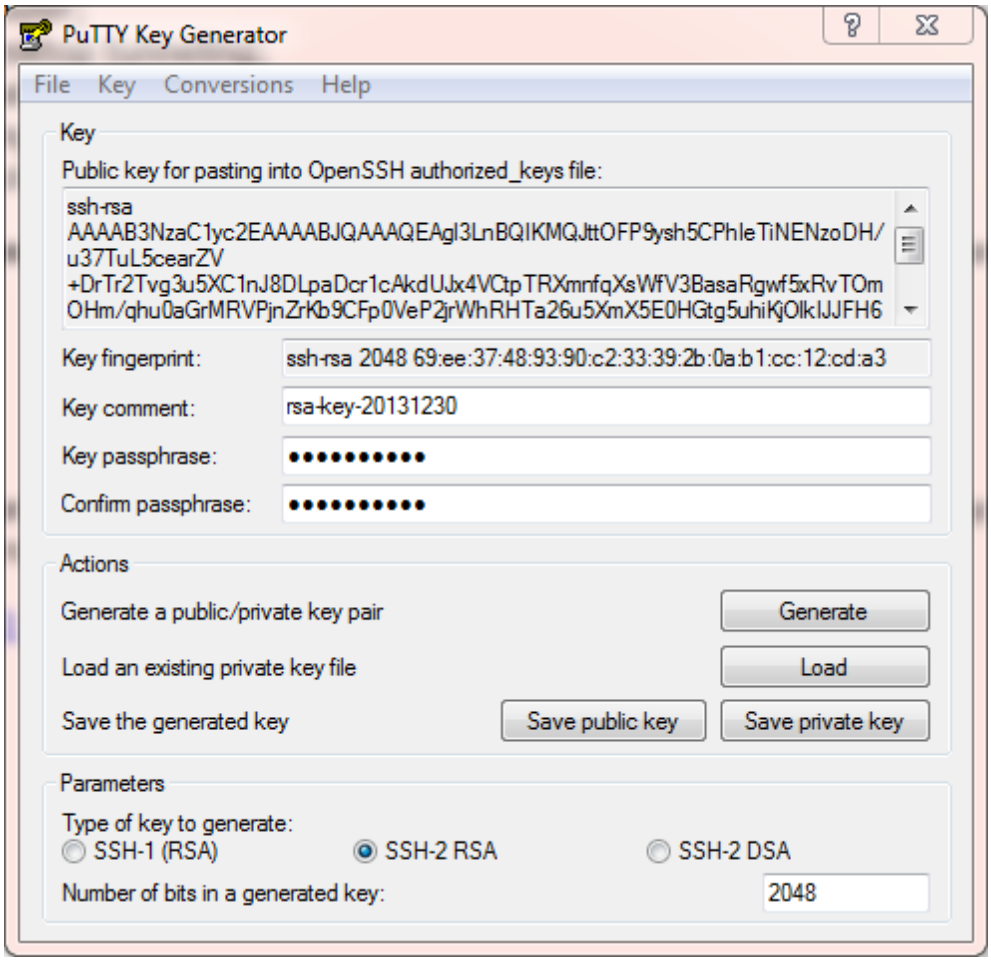
How do you create such a certificate? Here is one way:

The free secure shell program putty has the necessary tools. Download putty from www.putty.org When you install the program you will see several program installed on your computer.



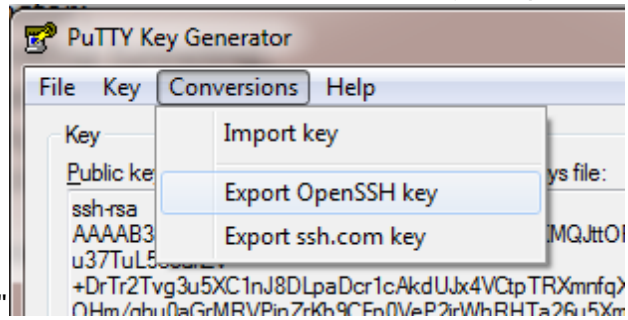
The programs and files that come with putty

One of the programs is puttygen.exe. This program creates the necessary keys. When you start it up, you can generate a key pair.



Creating a public/private key pair with puttygen

You can save the public and private keys separately as .ppk files but that is not what we need. But puttygen has also tool to convert the keys to pem files. The top menu has a tab "Conversions"



Converting the SSH key into a pem certificate

When we click on "Export OptnSSH key" we can then save the key with an .pem ending and that is it.

9.5 Using Encryption

9.5.1 About Encrytion

EDI Exchange supports the **Private Key Infrastructure** (PKI) encryption method. This type of encryption is the most generally accepted method of protecting EDI Files from being pried upon by unauthorized persons. Without going further into the details of PKI, Public-key encryption is a cryptographic technique which enables users to securely communicate on an insecure public network, and reliably verify the identity of a user via digital signatures. Read more in Private Key Infrastructure.

A public-key infrastructure (PKI) is a system for the creation, storage, and distribution of digital certificates which are used to verify that a particular public key belongs to a certain entity. The PKI creates digital certificates which map public keys to entities, securely stores these certificates in a central repository, and revokes them if needed.

A PKI consists of:

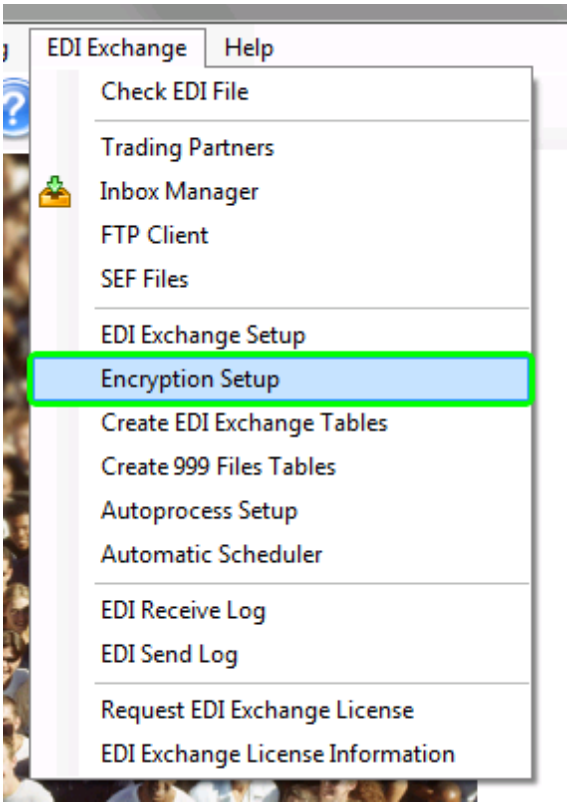
- A certificate authority (CA) that both issues and verifies the digital certificates.
- A registration authority which verifies the identity of users requesting information from the CA.
- A central directory is a secure location to store and index keys.
- A certificate management system.

EDI Exchange relies on other software to establish the PKI. It only uses the capabilities of these programs through their Application Programming Interface (API). You need to separately install either PGP Desktop or the open source GPG4Win programs and set them up with the public keys of your trading partners and your own private key.

9.5.2 Setting up Encryption

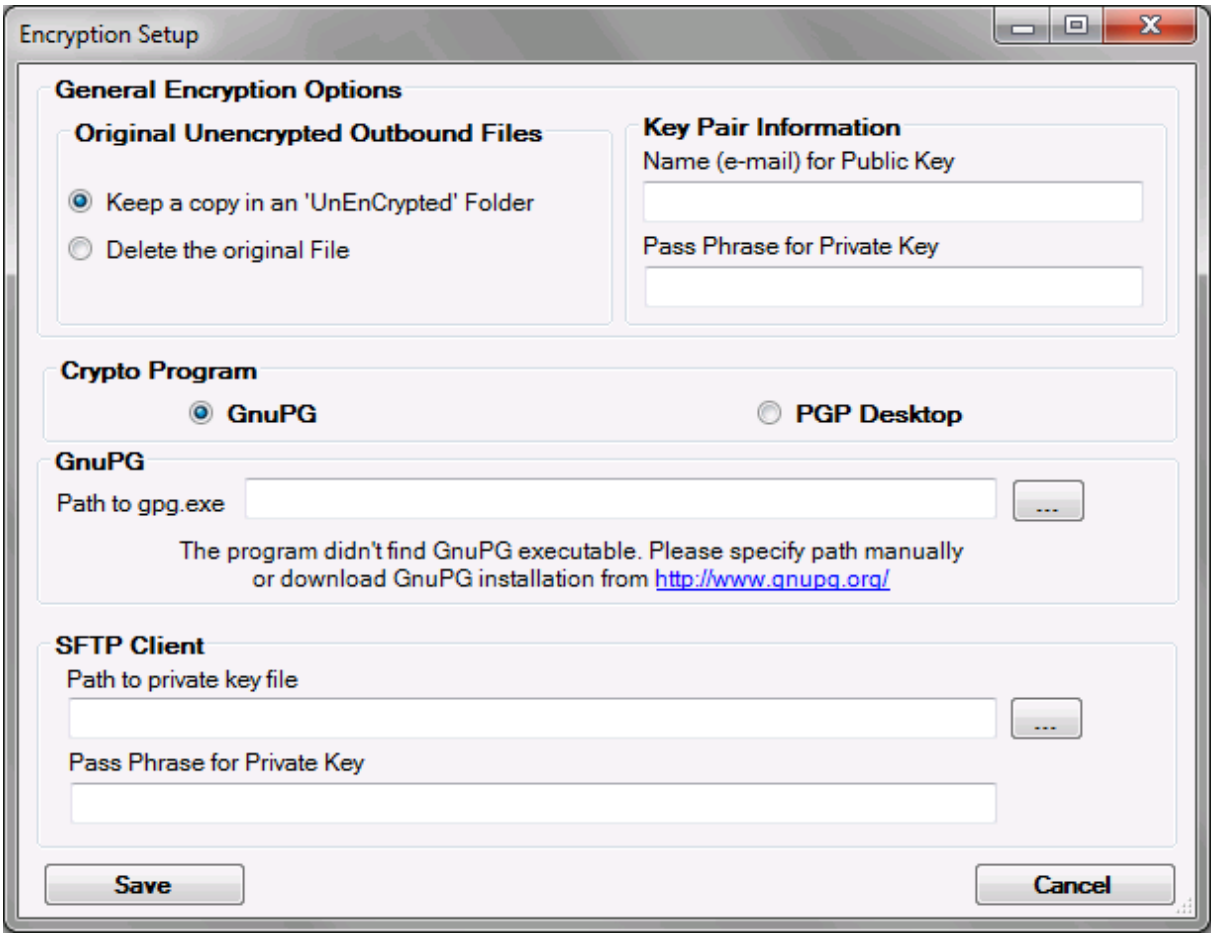
EDI Exchange allows you to set up the encryption for your EDI files. Follow the steps below.

1. Access the "Encryption Setup" window by selecting "Encryption Setup" under the "EDI Exchange" menu.



The encryption setup menu

2. The following window will appear.



The encryption setup screen

3. In this window define the following options:

General Encryption Options

- **Original Unencrypted Outbound Files**
  - **Keep a Copy in an 'Unencrypted' Folder** — When the HIPAAsuite program creates an EDI file for a trading partner that has selected encryption, you can keep an unencrypted copy in the "Outbox/*[trading partner]*/Unencrypted" folder. This is useful when you need to go back to the file and check on problems.

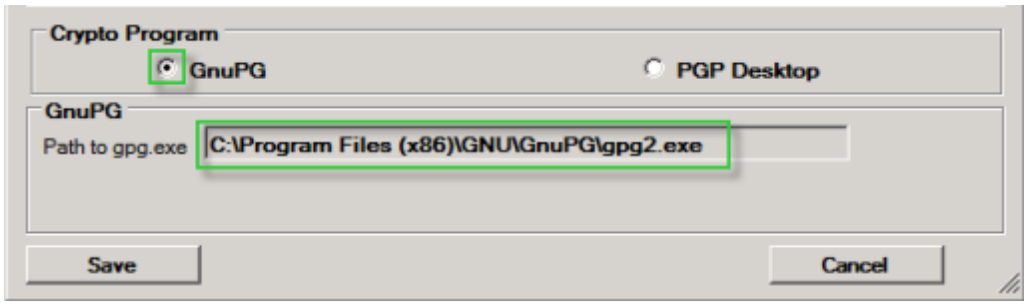
> Note: Once you encrypt a file with the public key of your trading partner, you will not be able to open it again. Only the owner of the private key can decrypt it and read it.

  - **Delete the Original File** — If you do not want to keep the unencrypted copy, select this option.
- **Key Pair Information**

- **Name (e-mail) for Public Key** – Enter name or e-mail that will be used to encrypt files for you by your trading partners.
- **Pass Phrase for Private Key** – Enter passphrase here to decrypt files encrypted previously with the pass phrase.

Note: The keys are identified by the email address of their owner.

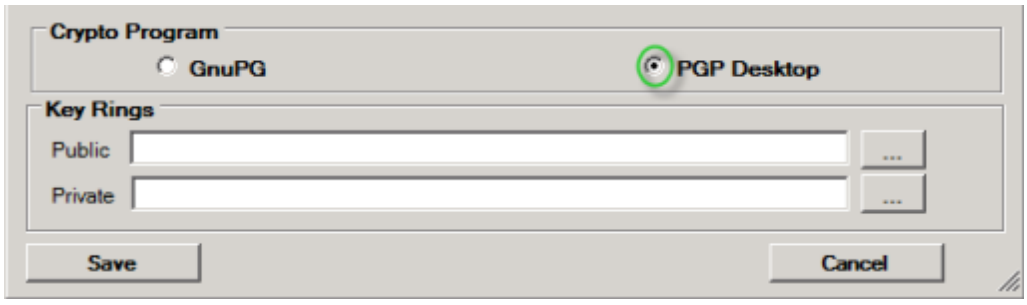
- **Crypto Program**
  - **GnuPG** – Select this option if you have already installed the GnuPG software and want to use it.



The configuration using GnuPG

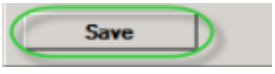
Note: When you select GnuPG, the program checks if the executable **`gpg.exe/gpg2.exe`** is present on your computer. If it is not found, you will have to specify the path manually or install the program first.

  - **PGP Desktop** – Select this option if you have already installed the PGP Desktop program and want to use it. You will see a different lower half of the screen, where you can indicate the location of the keys. PGP Desktop uses "key rings" – encrypted folders that contain all your keys. The location of these two files is very important for PGP Desktop.



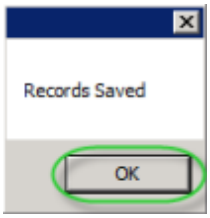
The configuration using PGP Desktop

4. Once the settings are done, click the "Save" button.



The "Save" button

5. The following notification will appear. Click the "OK" button.



Notification window

9.5.3 Using PGP Desktop

Pretty Good Privacy (PGP) is a data encryption and decryption computer program that provides cryptographic privacy and authentication for data communication. PGP is often used for signing, encrypting and decrypting texts, e-mails, files, directories and whole disk partitions to increase the security of e-mail communications. PGP and similar products follow the OpenPGP standard (RFC 4880) for encrypting and decrypting data. For more information, see How PGP works.

EDI Exchange supports PGP encryption and works seamlessly with PGP Desktop and open source Gpg4Win applications.

PGP Desktop (Symantec's encryption solutions) is a comprehensive suite of encryption applications which provides flexible, multi-layered encryption by bundling Drive Encryption to secure the files stored on local hard drives, and Desktop Email Encryption to secure confidential data in email. For more information, see PGP Desktop documentation.

PGP Desktop key features:

1. Hard drive encryption software locks down the entire contents of a laptop, desktop, external drive, or USB flash drive, including boot sectors, system, and swap files.
2. Enables encrypted email and secure AIM® Instant Messages.
3. Creates storage-independent encrypted containers for transport and sharing of specific files using included utilities; PGP Self-Decrypting Archive, PGP Virtual Disk, and PGP Zip.
4. Includes PGP Shredder which can completely destroy unwanted disk-based files and folders.
5. Drive Encryption can be centrally deployed and managed by Symantec Encryption Management Server.

PGP Desktop key benefits:

1. Secures email without burdening users, to improve compliance with policies and regulations without hindering productivity.
2. Allows users to easily and transparently share encrypted files and folders, improving data security without impacting user productivity.
3. Management by Encryption Management Server centralizes creation, deployment and management of data security policies and reporting.

PGP Desktop bundles the following products:

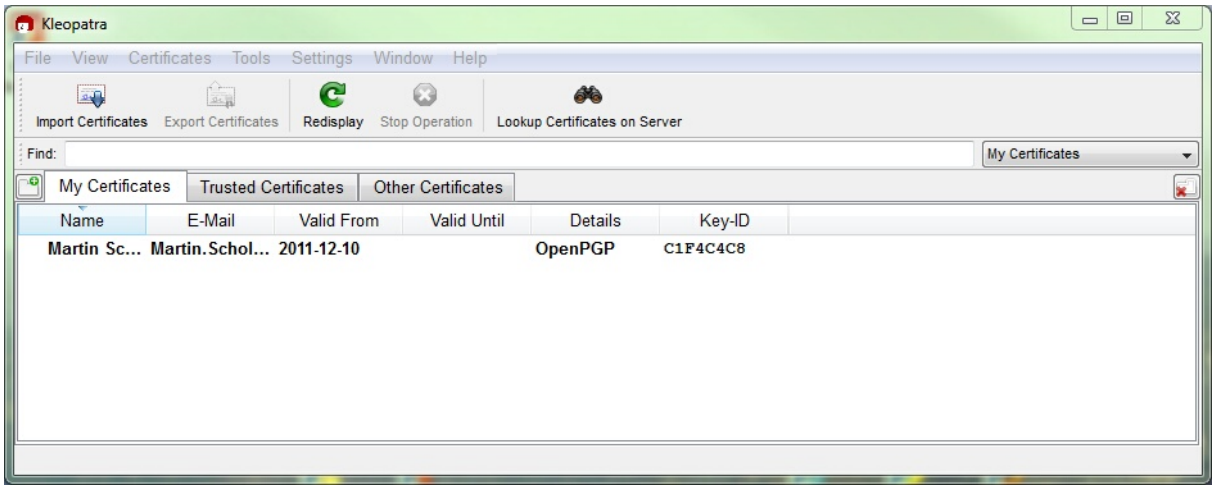
1. Drive Encryption. See System Requirements.
2. Desktop Email Encryption. See System Requirements.
3. Encryption Management Server. See System Requirements.

9.5.4 Using GnuPG

GnuPG is an Open Source project for the implementation of the OpenPGP (Pretty Good Privacy) protocols of encryption. GnuPG allows to encrypt and sign your data and communication, features a versatile key management system as well as access modules for all kinds of public key directories. GnuPG, also known as GPG, is a command line tool with features for easy integration with other applications. Front-end applications and libraries are also available. Version 2 of GnuPG also provides support for S/MIME.

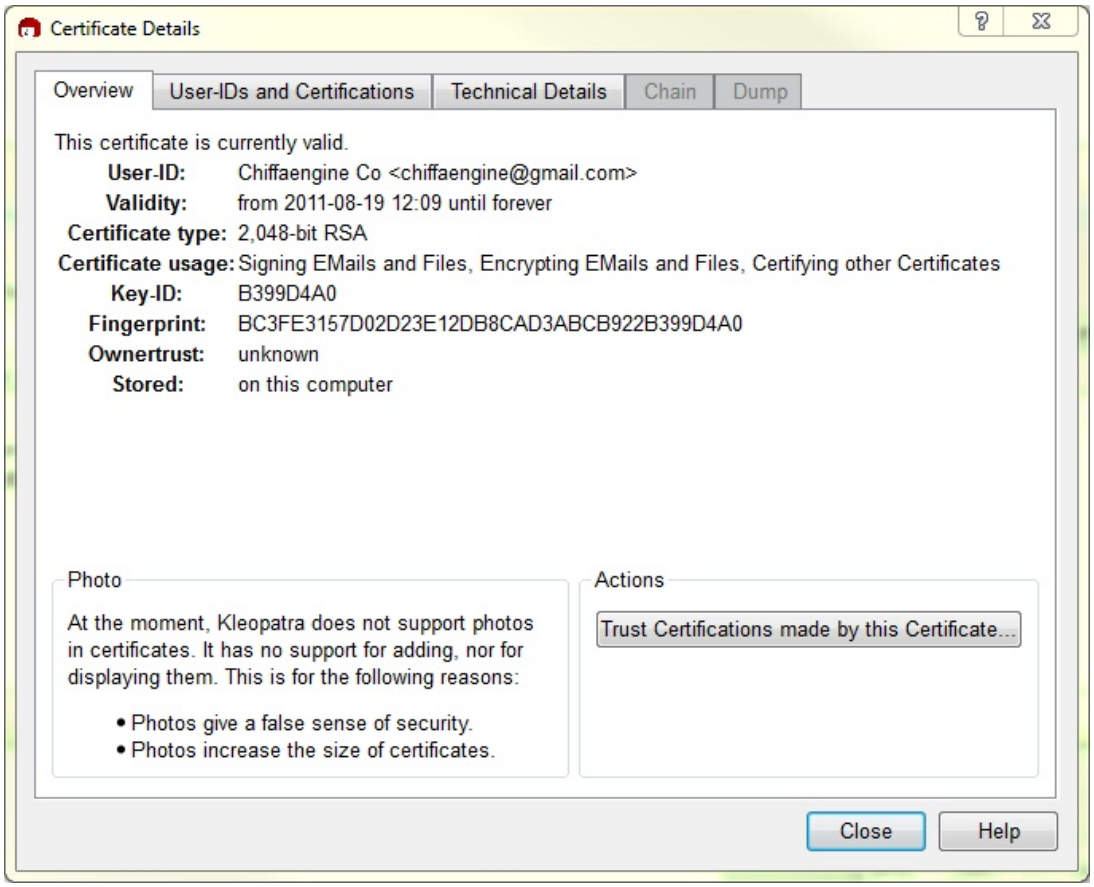
GnuPG is a free software, so it can be freely used, modified and distributed under the terms of the GNU General Public License.

We recommend Gpg4Win for encrypting of your files and emails. Gpg4Win supports both relevant cryptography standards, OpenPGP and S/MIME (X.509), and is the official GnuPG distribution for Windows. Gpg4Win contains Kleopatra as one of its Free Software components. For more information, see Gpg4Win documentation available both in PDF and HTML versions.



Kleopatra, a certificate manager for OpenPGP and X.509 (S/MIME) and common crypto dialogs

With Kleopatra, it is easy to manage your certificates and create your own ones. It seamlessly integrates with GnuPG. You can manage the key that you receive from your trading partners, because there is a screen to view the details of a key.



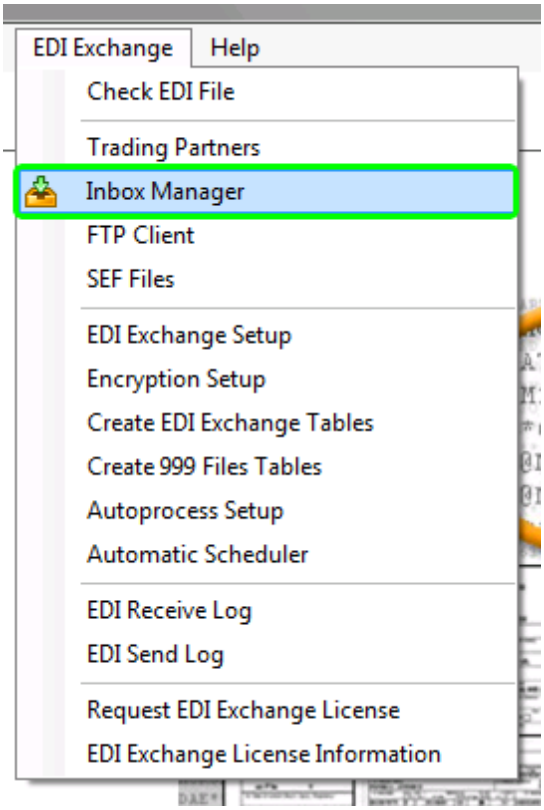
Certificate details with Kleopatra

9.6 Using EDI Exchange Features

9.6.1 Accessing Inbox Manager

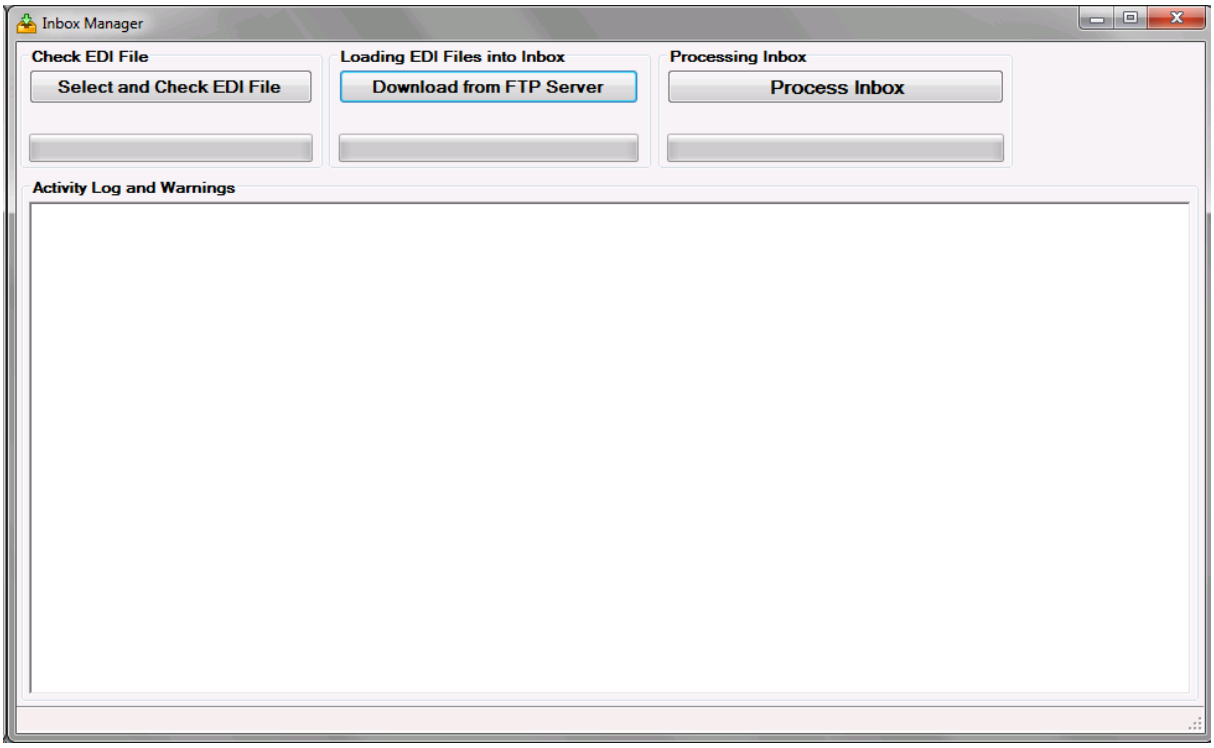
Using the Inbox Manager you can access the most important functions of EDI Exchange. Inbox Manager allows you to download EDI files into the "Inbox" folder and process these files. This screen handles the post-processing of the EDI files, their compliance check and auto-processing options.

1. To access the Inbox Manager, click the "Inbox Manager" under the "EDI Exchange" menu.



The "Inbox Manager" menu item

2. The following screen will come up.



The "Inbox Manager" window

Read more in:

- Downloading EDI Files From FTP Server
- Processing EDI Files
- Selecting and Checking EDI Files

9.6.2 Checking EDI Files

EDI file analysis based on the HIPAA standards. Compliance with HIPAA EDI rules is an essential part of the exchange of EDI documents. The standards are the only agreed upon rules that sender and receiver use to exchange data from completely different backend systems. Strict adherence is therefore necessary to guarantee frictionless operation.

Unfortunately, HIPAA compliance is difficult and the truth is that many HIPAA EDI files are truly bad. Syntax errors, omitted loops, missing elements, wrongly formatted elements — these are the most common EDI errors. Without a true analysis, it is difficult to say what data ends up in your system.

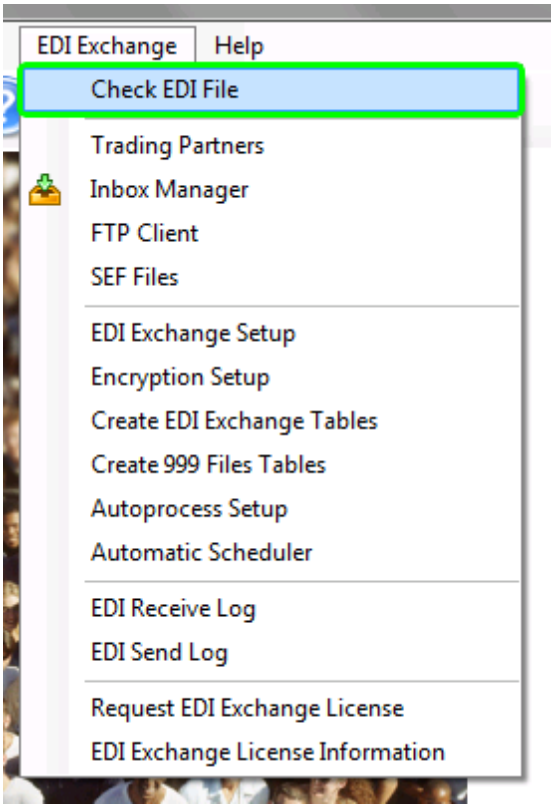
EDI Exchange has a built-in compliance engine that analyzes each incoming and outgoing EDI transaction. Line by line, element by element, error reporting provides a powerful tool to determine the quality of the incoming and outgoing EDI files. All HIPAA file versions are supported. The compliance check creates a detailed report that lists every

compliance issue. Outgoing files can also be checked and individual transaction in violation of HIPAA rules can be held back.

> Note: You can enable automatic compliance check on outgoing and incoming EDI files. See Setting up Incoming and Outgoing Files Options.

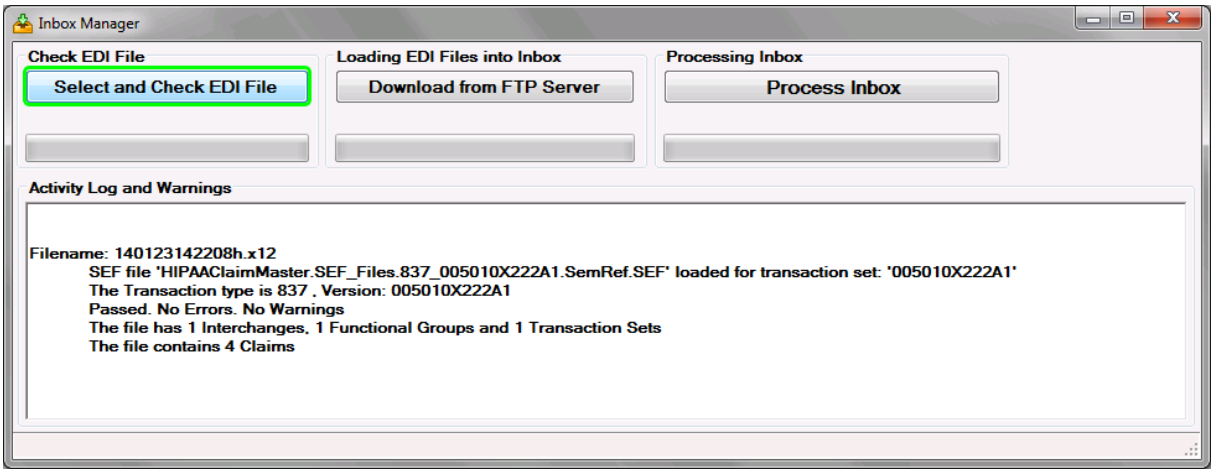
Follow the instructions below to check EDI files for compliance.

1. Select "Check EDI File" under the "EDI Exchange" menu item.



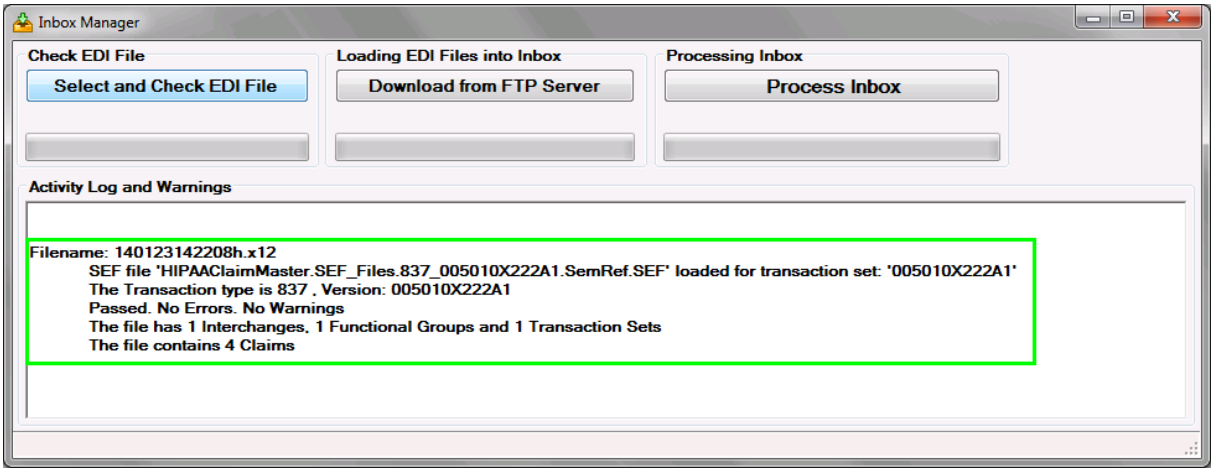
The "Check EDI File" menu item

Alternatively, you can click on the "Select and Check EDI File" button in the Inbox Manager window. Read more in Accessing Inbox Manager.



The "Select and Check EDI File" button

2. In the opened file selection dialog, select an EDI file and click "Open."
3. In the Inbox Manager, you can see the result messages for the operation. The details are displayed in the "Activity Log and Warnings" area.



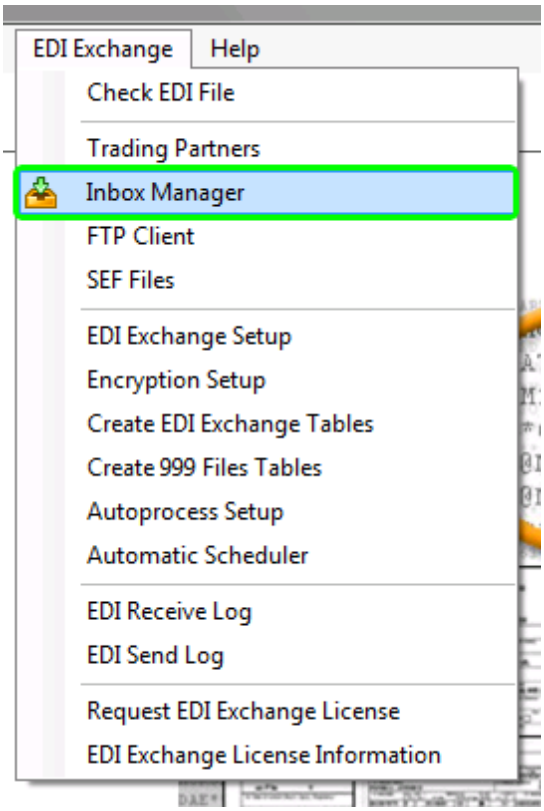
The "Activity Log and Warnings" area displaying log messages

9.6.3 Downloading EDI Files From FTP Server

EDI Exchange Inbox Manager allows you to load EDI files into the "Inbox" folder and process these files. Be sure you have setup FTP settings in the "Remote FTP" tab of the Trading Partner window (see Setting up Trading Partners).

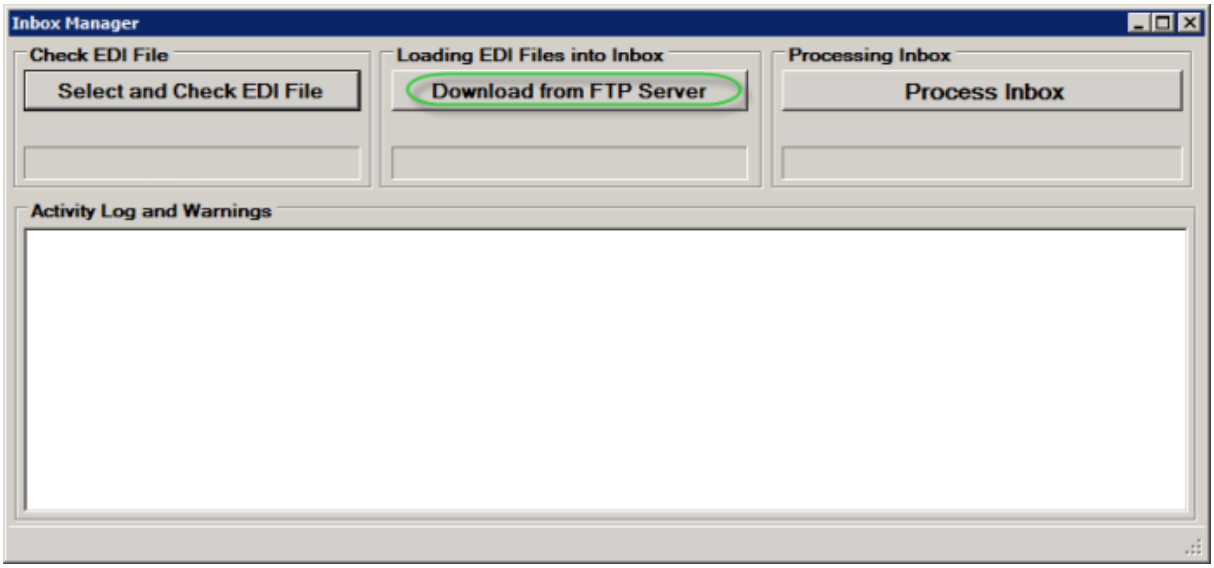
Follow the instructions below to upload EDI files into the "Inbox" folder.

1. Access the Inbox Manager by clicking the "Inbox Manager" under the "EDI Exchange" menu.



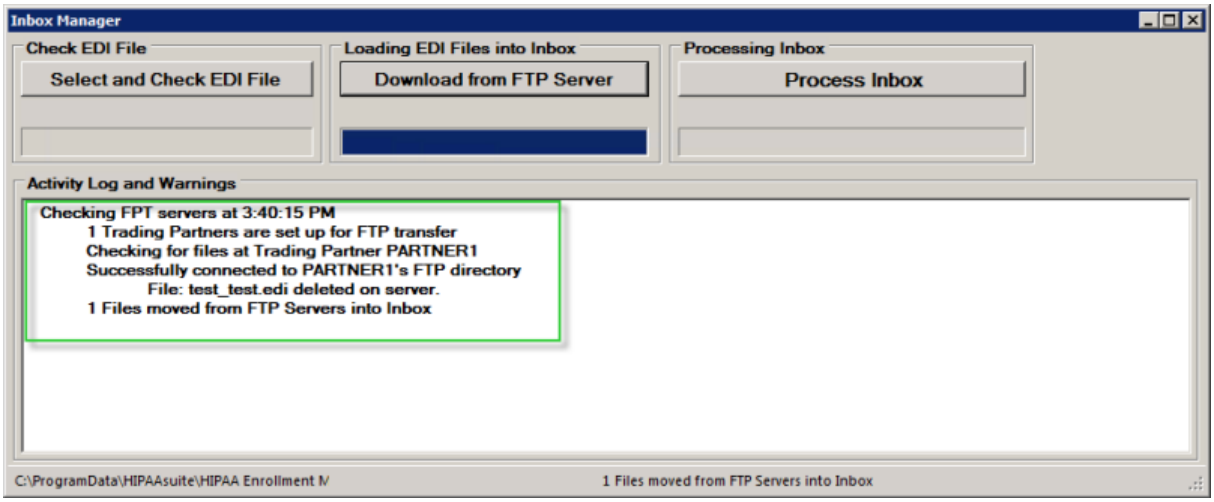
The "Inbox Manager" menu item

2. Click the "Download from FTP Server" button.



The "Download from FTP Server" button

3. When the process has been finished, the "Activity Log and Warnings" area displays the report.



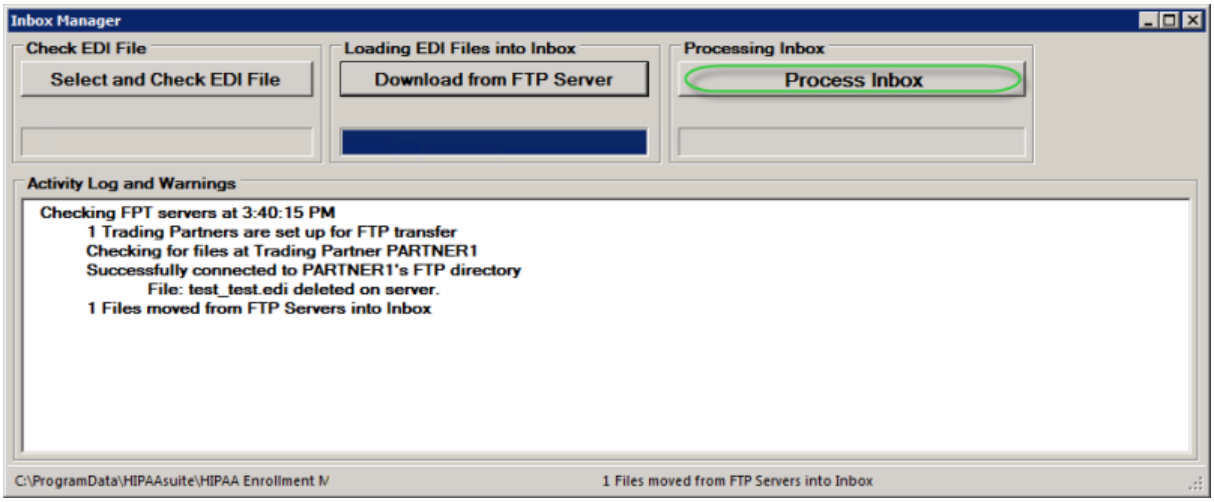
Activity Log and Warnings information

9.6.4 Processing EDI Files

EDI Exchange Inbox Manager allows you to process EDI files downloaded to the "Inbox" folder beforehand.

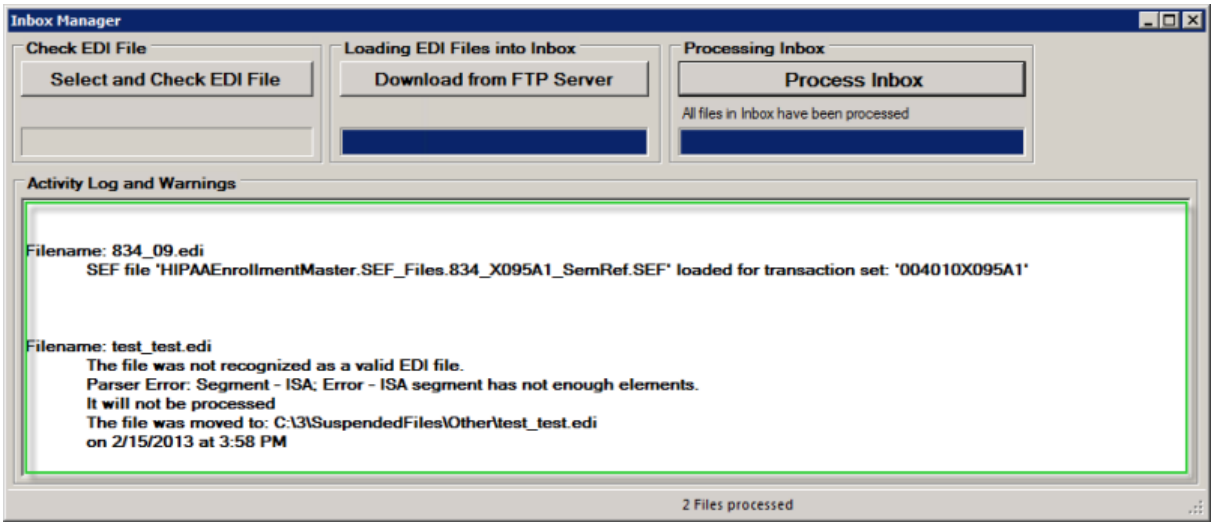
> Note: Once you have saved the auto-processing options (see Defining Auto-Processing Options), the files will not only be analyzed but also processed according to the defined settings. The auto processing enables you to combine and run multiple fulfillment steps together (for example, export, saving, printing.)

1. Once Downloading EDI Files From FTP Server is completed, and no errors are displayed, click on the "Process Inbox" button. This will autoprocess all files present in the EDI inbox directory.



The "Process Inbox" button

2. Once the processing is completed, review the Activity Log and Warnings information.

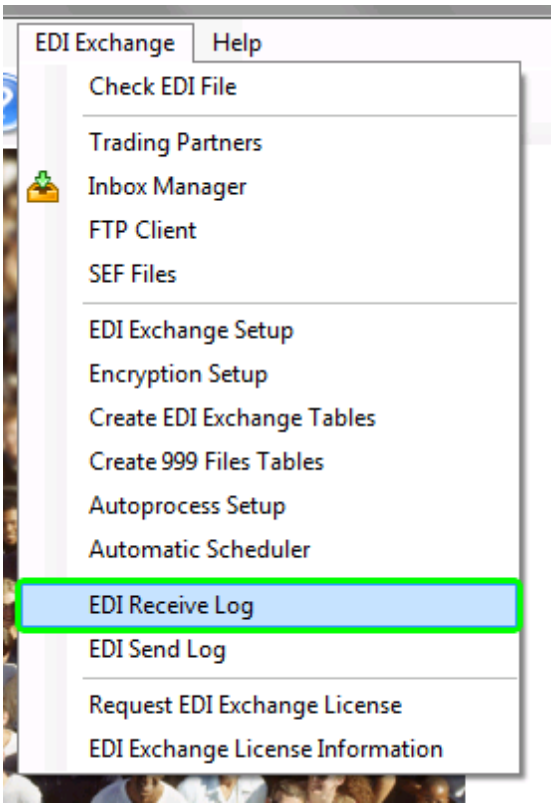


Activity Log and Warnings information

9.6.5 Accessing EDI Receive Log

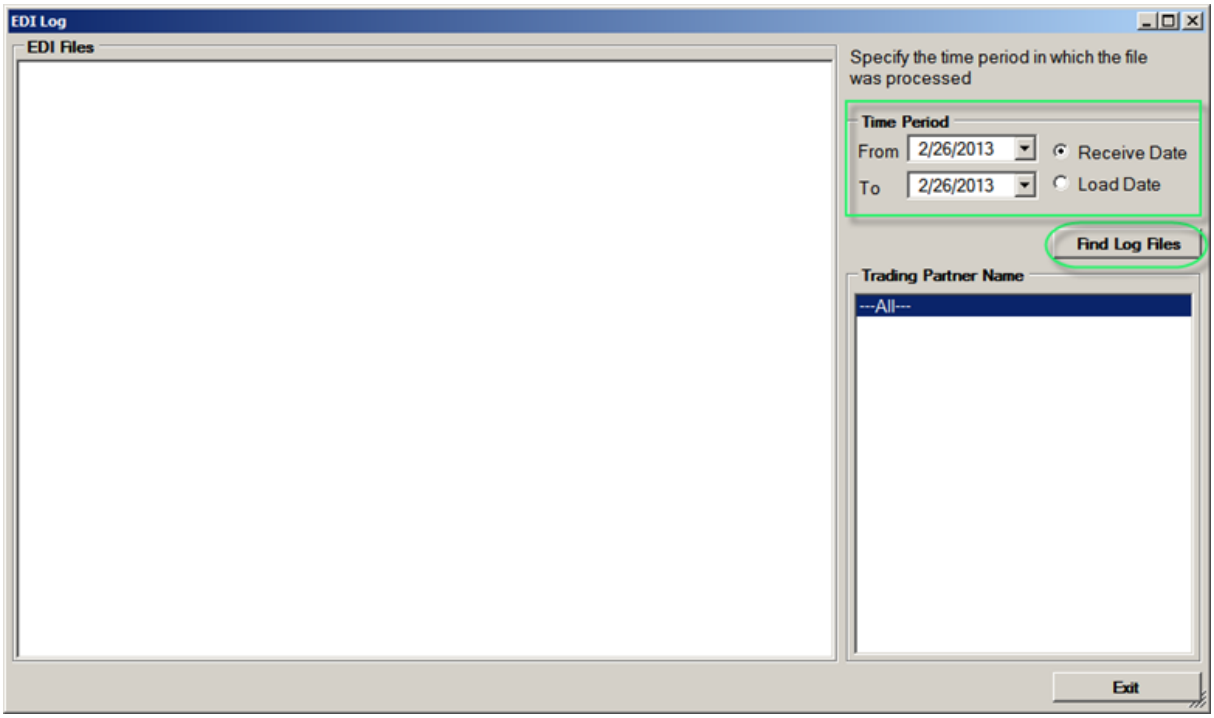
EDI Exchange has a file log. Each processed file creates an entry in the **Trans_Log** table. You can access the "EDI Log" window to query this table and see what files came in and how they were processed. You can access the EDI Receive Log once the application has been initialized. Follow the instructions below.

1. To open the "EDI Log" window, select "EDI Receive Log" under the "EDI Exchange" menu item.



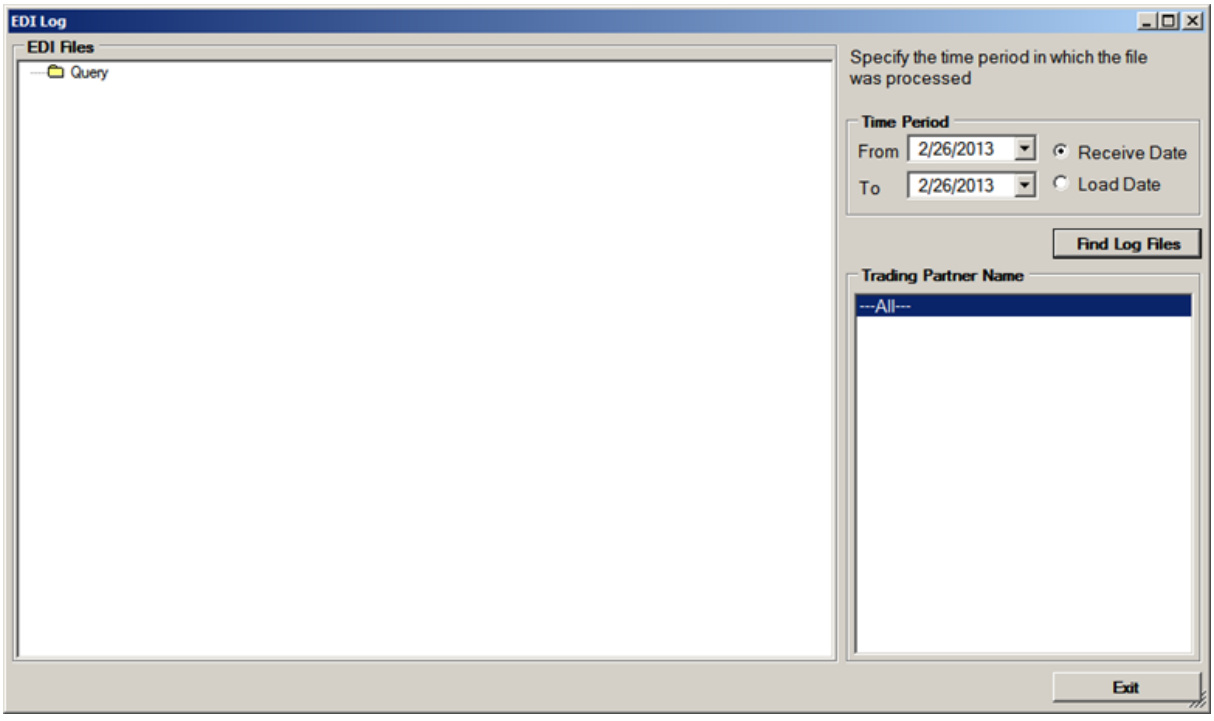
The menu for the EDI Receive Log

2. To display data, specify the time period and select trading partner.
    - **Time Period** — Period of time when the file was processed. Choose one of the available options:
        - **Receive Date**
        - **Load Date**
    - **Trading Partner Name** — You can select your trading partner from the list. If you select "---All---", all your trading partners will be included.
3. Click on the "Find Log Files" button to see the list of log files corresponding to your query.



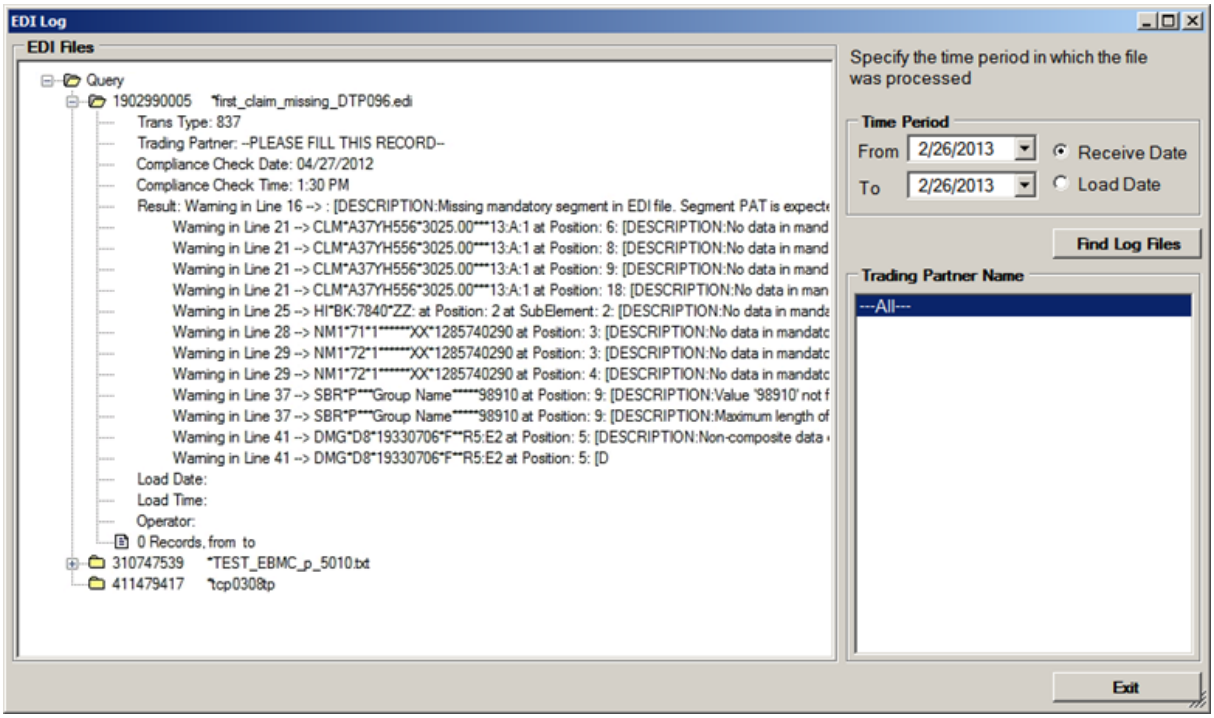
Specifying the time period

4. The log will be displayed in form of a tree.



Displayed log

5. You can open the folder icons and see details related to each file.



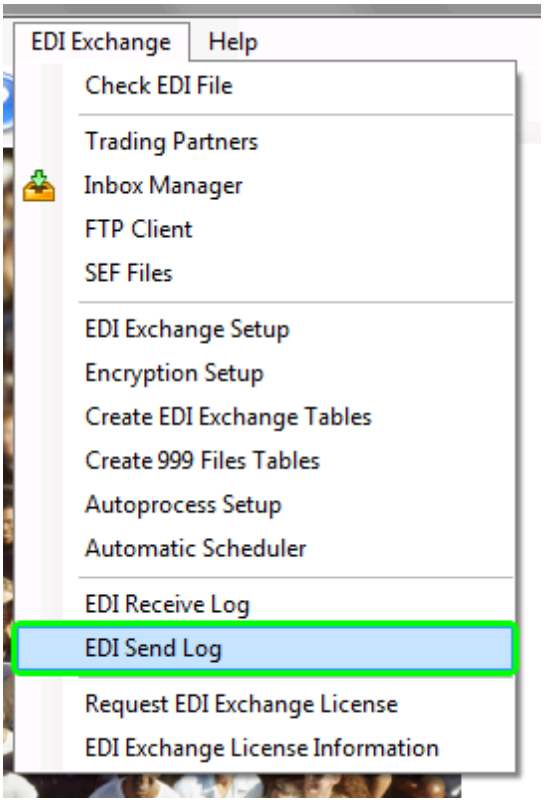
Details of the EDI Receive Log

If the records have been exported to the database, you can see the time, date and record count.

9.6.6 Accessing EDI Send Log

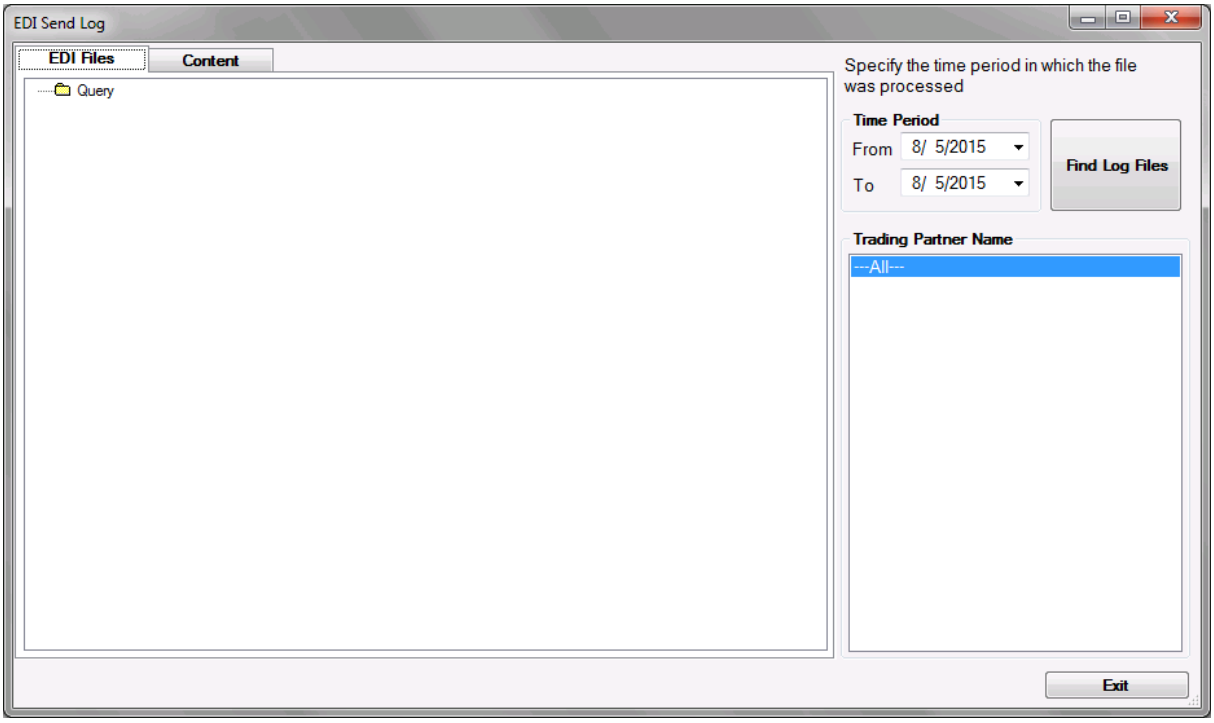
This page contains instructions on how to access the "EDI Send Log" window. It becomes available once EDI Exchange has been initialized.

1. Select "EDI Send Log" under the "EDI Exchange" menu.



The "EDI Send Log" menu

2. The following window will appear:



The "EDI Send Log" screen

3. To display the log data, select the time period and a trading partner.

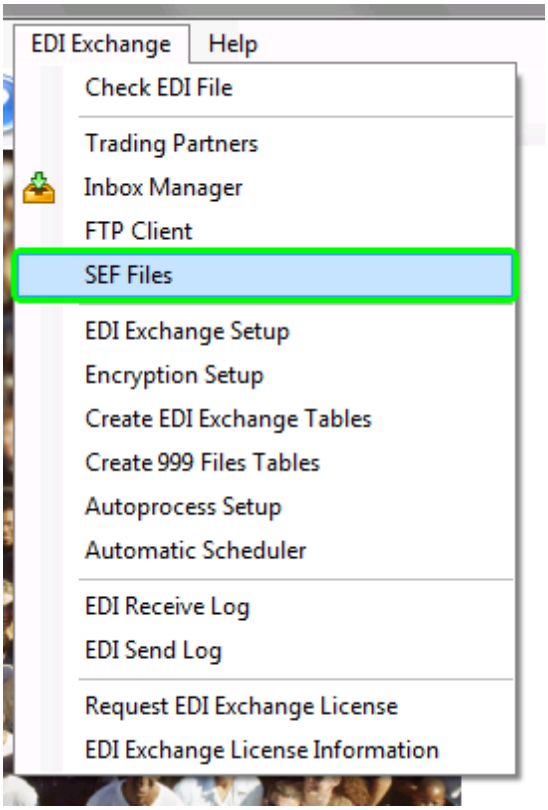
    - **Time Period** — Period of time when the file was processed. Choose one of the available options:
        - **Receive Date**
        - **Load Date**
    - **Trading Partner Name** — Select a trading partner in the list. If you select "---All---", all trading partners will be included.

4. Click on the "Find Log Files" button to display the list of log files corresponding to your query.

9.6.7 Listing SEF Files

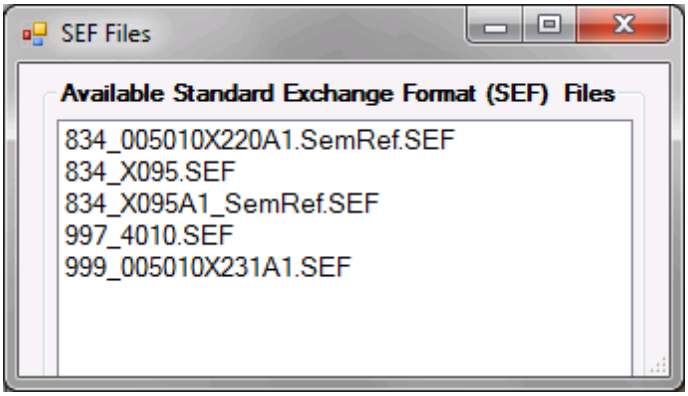
SEF (Standards Exchange Format) files are repositories of standards information that define the format of EDI documents. SEF files are the basis for the compliance check engine that EDI Exchange uses. These files contain all rules of the implementation guide of a transaction. There is a SEF file for each transaction that EDI Exchange is licensed for. For example, for 837 transactions we have SEF files for institutional, professional and dental claims in 4010, 4010A1 and 5010A1 version and the 997 and 999 transactions.

1. To access the list of available SEF Files, select "SEF Files" under the "EDI Exchange" menu.



The "SEF Files" menu item

2. The "SEF Files" window will appear.



A list of SEF files

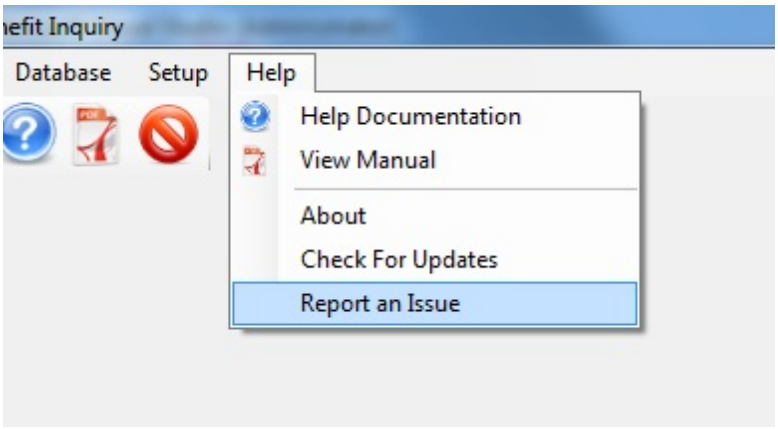
10 Issue Tracking

10.1 Reporting an issue

HIPAAsuite likes to make bug fixes fast and transparent. For this purpose we include a

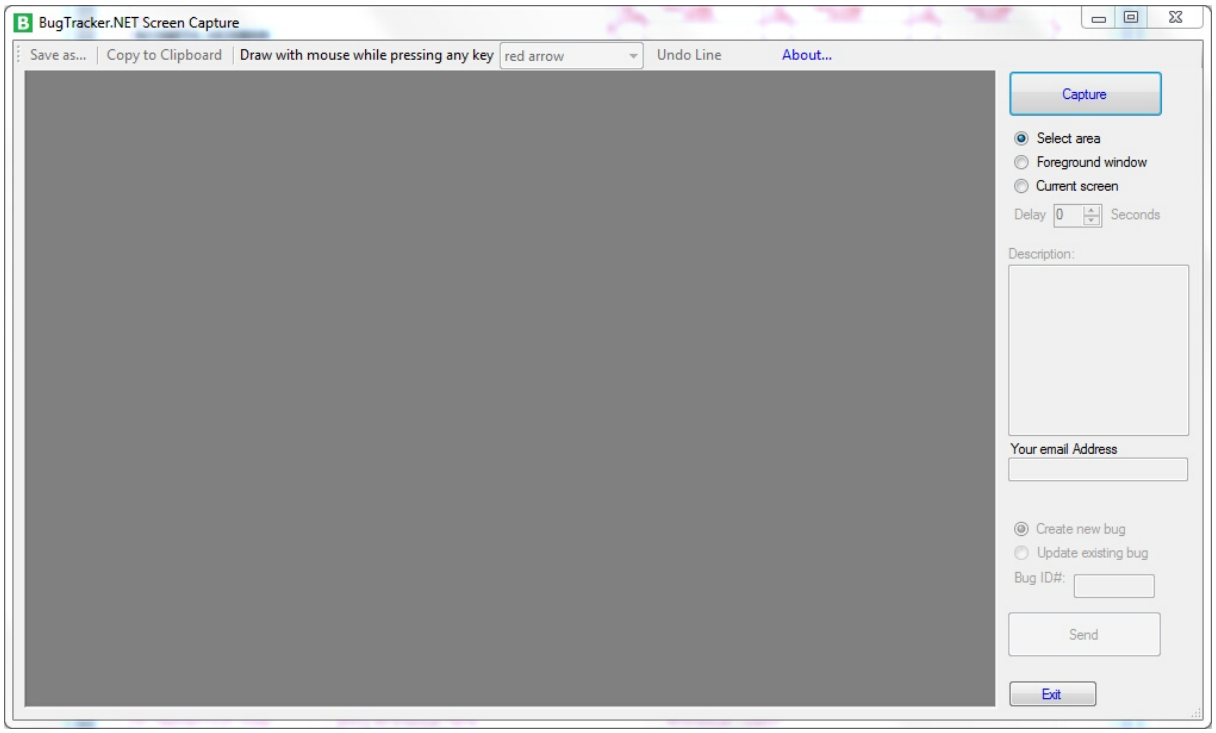
Bug tracker with the HIPAA Eligibility Responder. btnet, Bugtracker in ASP.Net is an open source project. HIPAAsuite implemented Bugtracker.Net in all its products to track bugs and enhancements. One of the reasons we liked btnet was the screen capture capabilities. We adapted and included this facility

You can reach the Issue Tracker under the Help menu



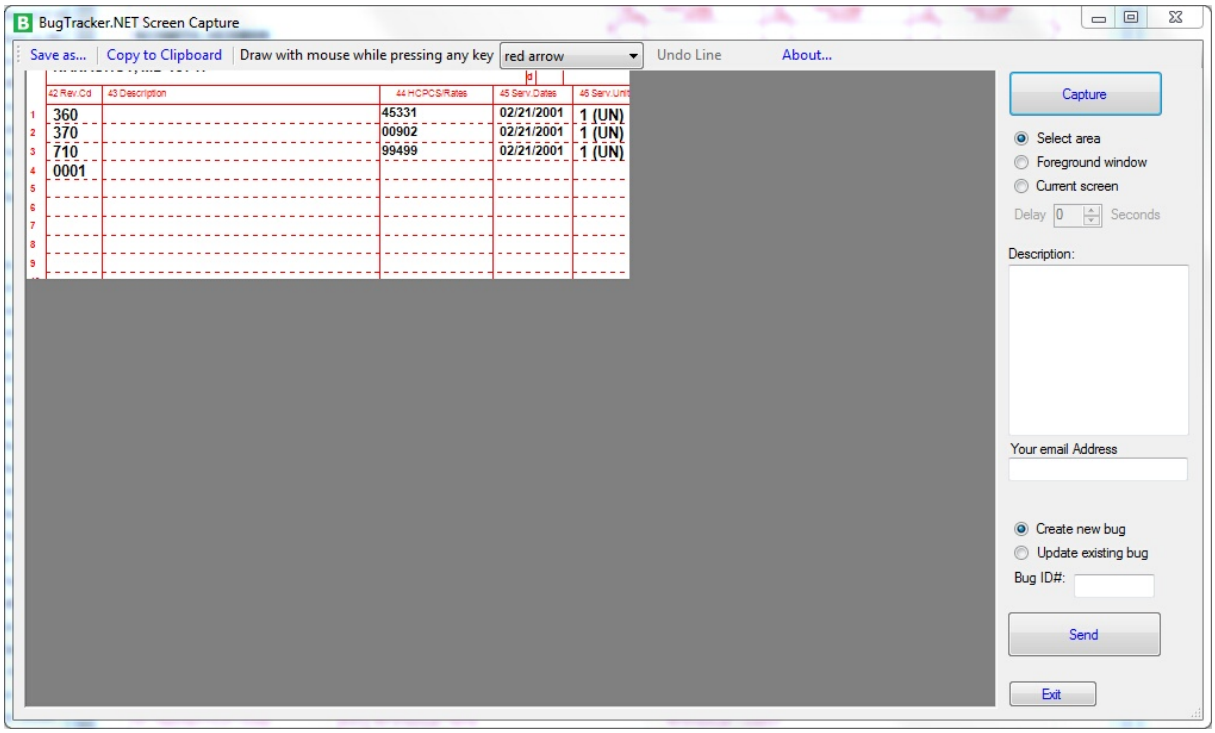
The menu for the issue tracker

Please remember the shortcut Ctrl + I to call the Issue tracker. Some screens do not give you access to the menu while they are open, but the key combination **Crtl + I** will call up the issue tracker report screen.



The BugTracker.Net screen capture facility

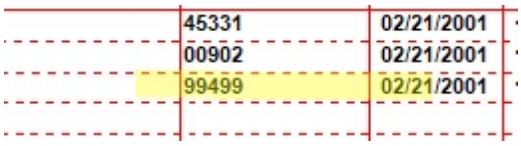
If you click on 'Capture' you can snap a picture of your screen



With a section from the underlying screen

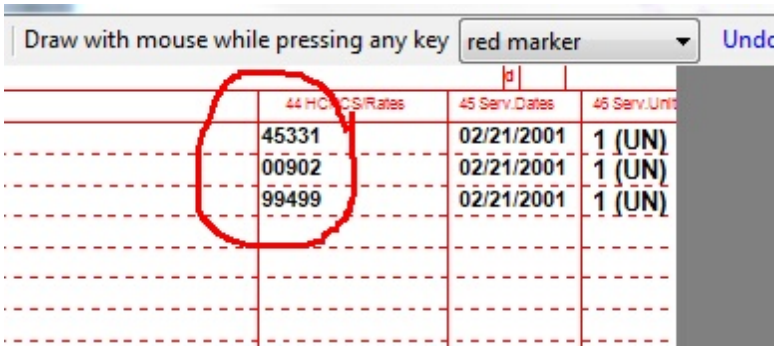
Enter as much information into the description as possible. You can enhance your screen shot with drawings. By pressing any key and holding down the mouse while over the canvas, you either highlight in yellow, free draw in red or make red arrows:

You can high light sections



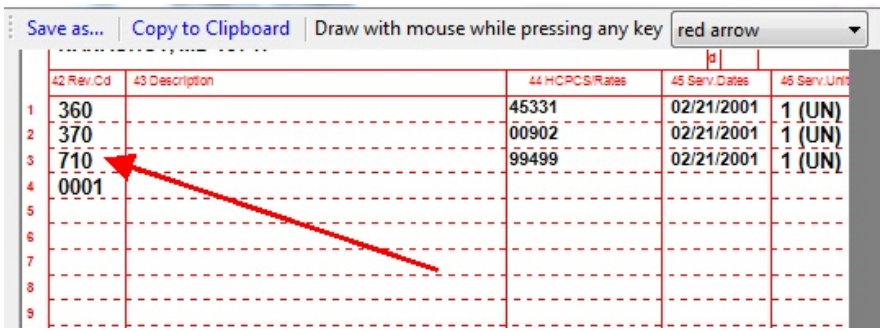
High lighting a section

You can draw circles



Circling a section

You can point arrows to pinpoint your concerns



Drawing an arrow

Now please enter your email address so that we can get in contact with you and indicate whether this is a new bug or a follow up on an existing issue. Then click on 'Send'

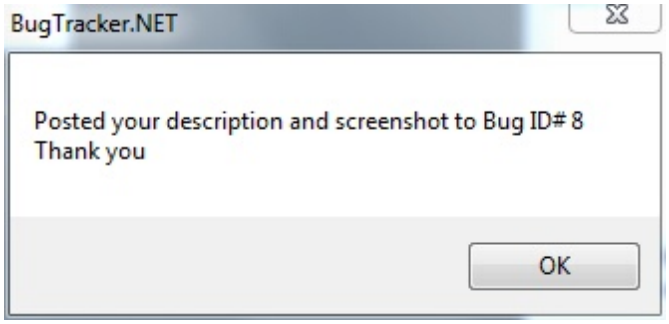


Figure 7: Acknowledgement of Issue submission

Now this bug has been submitted, we will be notified by email and you will get updates on the issue.

Back Cover