State of Illinois Healthcare and Family Services

ASC X12N (005010X221A1)

Healthcare Claim Payment/Advice

CORE 835 Master Companion Guide

Disclosure Statement

The information in this document is subject to change. Any revisions will be posted on the Department's web site (Chapter 300 Companion Guide 5010 - Electronic Processing | HFS (illinois.gov)).

Preface

The Health Insurance Portability and Accountability Act (HIPAA) requires all covered entities to comply with the HIPAA EDI standard transactions adopted under this Federal Regulation. The purpose of this 835 Companion Guide to the v5010 ASC X12N Technical Report Type 3 (TR3) is to clarify and specify the data content when exchanging electronically with State of Illinois Healthcare and Family Services (SOI-HFS). This Companion Guide is intended to convey information that is within the framework of the ASC X12N TR3s adopted for use under HIPAA. The Companion Guide is not intended to convey information that in any way exceeds the requirements or usages of data expressed in the TR3.

1 Table of Contents

This page intentionally left blank so the primary page of this document may begin on a right-hand page.

1   INTRODUCTION

This document describes what is required to consume the State of Illinois Healthcare and Family Services (SOI-HFS) CAQH CORE 835 web service. This document follows the CAQH CORE Phase III guidelines.

1.1   SCOPE

Covered entities (payers, health care providers, health plans and clearinghouses) must comply with the ASC X12N 835 (005010X221A1) TR3 for transmission of Electronic Funds Transfer (EFT) and Electronic Remittance Advice (ERA). Our companion guide defines CORE Business rules for 835 data content, response times, connectivity, and system availability. This document should be used to supplement the X12N 835 TR3.

1.2   OVERVIEW

In January 2012, the U.S. Department of Health & Human Services finalized the first regulation on operating rules for eligibility and claim status transactions. Effective January 1, 2013, the Affordable Care Act (ACA) mandates adoption of the rules for Health Insurance Portability and Accountability Act (HIPAA) electronic data interchange (EDI) transactions. In July 2012, the second set of operating rules was published for Electronic Funds Transfer & Electronic Remittance Advice. The compliance date is January 1, 2014. This standard companion guide is part of the CAQH CORE Operating Rules adopted under this Federal Regulation.

1.2.1   What is CAQH?

The Council for Affordable Quality Healthcare (CAQH) is a cross-section of industry representatives from health plans, provider networks, and Health Insurance Industry associations. This non-profit alliance came together to provide a variety of solutions aimed at streamlining and simplifying health care administration.

1.2.2   What is CORE?

The Committee on Operating Rules for Information Exchange (CORE) was created by CAQH to author a set of Operating Rules that would help the industry meet requirements not currently defined in the x12 TR3. These include data content rules and infrastructure rules.

1.2.3   What is CORE Certification?

Any entity that creates, transmits, or uses eligibility or claim status data is eligible to become CORE-certified. CORE-certification indicates an entity has signed the CORE Pledge and successfully completed certification testing, both of which are designed to demonstrate an entity's compliance with all the CORE rules. Certification is voluntary and may be done for Phase I, II & III separately or concurrently. For more information, go to www.caqh.org.

1.3   REFERENCES

1.3.1   The ASC X12 5010 version of the HIPAA TR3s can be purchased at:

http://www.wpc-edi.com/

1.3.2   SOI-HFS's provider portal:

https://www2.illinois.gov/hfs/MedicalProviders/xxEDI/medi/Pages/GettingStarted.aspx

1.3.3   CAQH/CORE information can be found on their website:

http://www.caqh.org/ORMandate_EFT.php

1.3.4   **WSDL:** http://www.w3.org/TR/wsdl

1.3.5   **SOAP:** http://www.w3.org/TR/soap/

1.3.6   **CORE XML Schema:** http://www.caqh.org/SOAP/WSDL/CORERule2.2.0.xsd

1.4   ADDITIONAL INFORMATION

This Companion Guide is intended for professionals who are involved in implementing EDI solutions for health care providers, such as vendors of practice management software, and service providers such as claims clearinghouses who send EDI on their clients' behalf. As such, this Companion guide assumes a working knowledge of ASC X12, its structure and nomenclature, and implementing or supporting different methods of connectivity. It also assumes a working knowledge of the 835 transaction as described in the Technical Report Type 3 (TR3).

- Submitters must have a secure internet connection (HTTPS) capability to submit a CORE 835 retrieval request and receive 835 responses.
- Only batch 835 retrieval requests and responses are supported.

2   GETTING STARTED
2.1   WORKING WITH SOI-HFS

SOI-HFS offers HIPAA X12 EDI via two types of connections:

1) Medical Electronic Data Interchange (MEDI) web site (https://).

   a. MEDI is a web portal that provides access to many other web sites to allow trading partners to conduct many different types of online business with SOI-HFS. MEDI also tracks and maintains all of SOI-HFS' trading partner accounts, their respective account types (Medicaid provider, payee, other government payer, and other business), the MEDI users authorized to be an account's Administrator (Admin), the MEDI users authorized to be an account's employee(s) and/or submitter(s), and each account's authorized payee (the payee authorized to download 835 electronic remittance advices for the accounts whom have given them authorization within SOI Medicaid).

   b. MEDI is oriented towards human user interaction (MEDI is not a business-to-business [B2B] architecture, however a B2B connection offering is available and is discussed below) allowing access to many different web applications. Specifically, the Internet Electronic Claims (IEC) web application allows users to perform EDI transactions via file uploading/downloading to/from the MEDI-IEC portal. Access to MEDI requires a Digital ID for the login credentials (username and password). A Digital ID is issued to an individual using their identity (an identity-proofing service is utilized to verify identity) and not to an organization, business, institution, or company. MEDI users are individuals, not businesses. Once a MEDI user has their Digital ID, they can establish a new MEDI account, request authorization to become an Admin of an existing account, request authorization to become an employee/submitter of an existing account, etc. All these relationships/authorizations between various MEDI users and MEDI accounts is tracked and maintained by MEDI. It would not be possible for someone at a trading partner to get access to another user's Digital ID as that would be considered a form of identity theft and a violation of SOI security policy. Each person who uses MEDI must acquire their own Digital ID using their own identity to access MEDI.

2) CAQH CORE web service portal (business-to-business [B2B] architecture).

   a. Use of the web service portal requires the Payee to establish their required account within MEDI under their assigned Payee ID because the web service uses the authorizations from MEDI to secure 835 files. Only those Payees with an account within MEDI can download 835 files via the web service. Likewise, clearinghouses (and any other business entity) wanting to be able to download 835 files on behalf of a Payee, those entities must set up their MEDI account and request authorization from the Payee in MEDI. Once the account is created and the authorization completed, the clearinghouse will be able to download 835 files for the Payee.

2.2   TRADING PARTNER REGISTRATION

MEDI Registration and Authorization

If you are already a registered MEDI user and have all necessary authorizations already in place within MEDI, you

can skip this <u>MEDI Registration and Authorization</u> step and move forward to establishing your access to the CAQH CORE web service portal by following the steps outlined below in <u>CAQH CORE Web Service Portal Registration</u>.

To become a MEDI user, please go to the MEDI Home web page URL (<u>https://hfs.illinois.gov/medicalproviders/edi/medi.html</u>), then use the left-hand side menu link labeled **MEDI Help (.PDF)** to download the instructions manual. This manual provides specific instructions on how to set up your own MEDI account and how to acquire the authorizations necessary, depending on what type of business, to perform business electronically with SOI-HFS. The MEDI Home web page also has other useful menu links to help you get started (links such as MEDI FAQ, Getting Started, Registration, etc.) using MEDI.

Steps for Clearinghouse or Billing Service to request Payee Authorization

After completing the steps outlined in the MEDI Help document to establish your account within MEDI, the following steps are required of the Clearinghouse and/or Billing Service to request authorization from the payee to perform business on behalf of that payee within MEDI using the CAQH CORE Web Service 835 download function.

Step 1: Use the **Req Payee Auth** button from the Business Authorization Menu page.

Step 2: Enter the payee information and click submit.

Steps for Payee approving Authorization requests from Clearinghouse or Billing Service

After the Clearinghouse and/or Billing Service has completed submitting their authorization request within MEDI to the payee, the following steps are required of the payee to approve the authorization request from the Clearinghouse and/or Billing Service to perform business on behalf of that payee using the CAQH CORE Web Service 835 download function.

Step1: Click on the **Business Auth** button from the Payee Authorization Menu page..

Step2: Click on the appropriate radio buttons to either ACCEPT or REJECT requests, then click the Submit button.

Step3: Success page will be displayed.

CAQH CORE Web Service Portal Registration

Trading partners desiring to exchange EDI transactions with SOI-HFS using a B2B type connection need to perform the following steps:

1) First, as stated above, establish an account in MEDI and request the required authorizations from other MEDI entities as outlined above. If you already have a MEDI account and the proper authorizations established, you can skip this step. If not, this first step is crucial toward establishing the ability to utilize the CAQH CORE web service because the web service utilizes/leverages the authorizations recorded within MEDI as the mechanism to secure 835 files from being downloaded via the web service by only those entities (such as a clearinghouse and/or billing service) authorized by the payee (the clearinghouse and/or billing service could have authorizations from many payees). Clearinghouses who want to download 835 files for a payee must establish their MEDI account as an Other Business, then request authorization from the payee within MEDI. Once the payee has approved that request, the clearinghouse will have the authorization to download 835 files for that payee. Once authorization within MEDI is completed, then move to the following second step.

2) Second, contact SOI-HFS to request a SOI-HFS Trading Partner Application and Trading Partner Agreement, complete both documents, and return them to SOI-HFS for processing. Even if you are already authorized to connect to the web service, you must complete this step because the addition of the 835 download functionality to the web service has required SOI-HFS to make programming changes within MEDI and the CAQH CORE Web Service to ensure only authorized entities can download 835 files. Simply contact SOI-HFS Bureau of Technical Support at: HFS.EDITradingPartner@illinois.gov to request CAQH CORE Web Service Trading Partner Application and Agreement. Return your completed documents to the same email address.

Depending on what type of transaction(s) you desire to transact with SOI-HFS through the web service will determine what documentation/authorizations are required. However, once all documentation/authorizations are completed and approved, you will receive the necessary information on how to connect to the web service (which will include the URL).

It should be noted, the payee has the authority to retract their approval/authorization at any time by revoking a clearinghouse and/or billing service's authorization at any time within MEDI. The revocation within MEDI would immediately remove a clearinghouse or billing service's ability to download 835 files on their behalf. It is the payee's responsibility to administer their MEDI account and manage what other MEDI accounts/entities have access to perform business within MEDI on their behalf.

2.3 CERTIFICATION AND TESTING OVERVIEW

There is no formal certification and testing for 835 HIPAA transactions since it is an inquiry/response (non-update) transaction.

3   TESTING WITH THE PAYER

Although there is no formal testing, SOI-HFS recommends submitting at least one request transaction to ensure connectivity and data transfer is successful.

Listed below are steps to follow:

- Obtain your SOI Digital ID (username/password) for MEDI.

- Create your MEDI account and request authorization(s) from other MEDI accounts for which you are to perform electronic business. Payees must be authorized within SOI Medicaid by providers, physicians, pharmacists, pharmacies, etc. as their official payee in order to have the ability to download the 835 file. Likewise, clearinghouses must have a MEDI account that has been authorized by the Payee before they can download an 835 for that Payee.

- Register to use the SOI-HFS CAQH CORE web service and receive your CAQH CORE web service username and password.

- Create 835 retrieval request based on CAQH CORE specifications and SOI-HFS user instruction documentation supplied when successfully registered as a trading partner with permissions to consume the CAQH CORE web service.

- Submit initial request to SOI-HFS CAQH CORE web service.

- Receive 835 response and review content to determine production readiness.

4   CONNECTIVITY WITH THE PAYER/COMMUNICATIONS PROCESS FLOWS
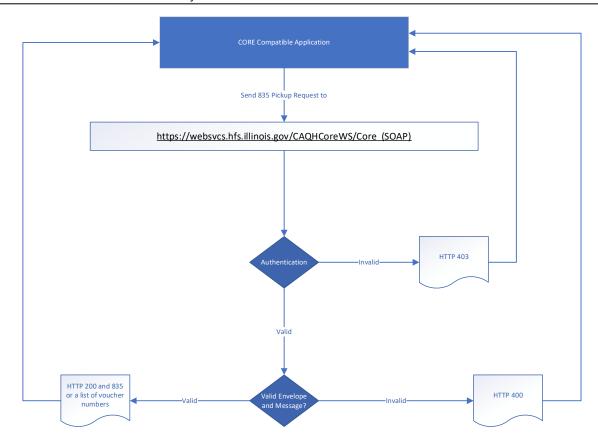### 4.1   SOI-HFS CORE System Availability

Normally processing is 24 x 7 x 365, however maintenance may occur between Saturday 10pm – Sunday 8am (CST).

All scheduled downtimes will be posted to the MEDI Login web page and emergency downtimes will be noted there as well.

4.2   Process Flows

4.2.1   Batch Pickup

4.2.1.1   SOAP Request and Response

1. STEP 1 - 835 Request/Response:

Overview of Process Flow Instructions:

1. The user application submits a batch pickup SOAP request to:
   https://webservices.soi-hfs.com/CORE/ServiceReference.svc/batch.

2. SOI-HFS's system will authenticate client credentials. If unable to authenticate, then an HTTP 403 Forbidden response is returned.

3. SOI-HFS's system will validate username and password and other elements of CORE envelope metadata. If validation fails, HTTP 400 status response is returned.

4. If the user is successfully authorized and envelope validated, SOI-HFS will deliver the response transaction(s), as appropriate for Payload Type. If no match occurs, HTTP 400 status response is returned.

5. If the request payload contains Payee ID and Voucher Number the web service attempts to retrieve the specific 835 for the voucher number and return the 835 X12 file in the response payload. If any other request payload data fields are also populated, they will be ignored.

6. If the request payload does NOT contain a Voucher Number, the other submitted search criteria specified in the request payload are used to return a list of voucher numbers which meet the criteria in the response payload. In the event no vouchers are found for the supplied criteria, an ErrorCode "NotFound" and an ErrorMessage "No records found for supplied search criteria" is returned.

Detailed Process Flow Instructions:

1) Example WSDL Format for X12_835_Request_005010X221A1, the actual values within the below tags would be specific to your entity with exception to the ReceiverID, it will always be 37-1320188 for SOI-HFS:

<wsse:Security>

<wsse:UsernameToken>

<wsse:Username>username</wsse:Username>

<wsse:Password>password</wsse:Password>

```
    </wsse:UsernameToken>
  </wsse:Security>
  <cor:COREEnvelopeBatchSubmission>
    <PayloadType>X12_835_Request_005010X221A1</PayloadType>
    <ProcessingMode>Batch</ProcessingMode>
    <PayloadID>6a3540fc167151</PayloadID>
    <PayloadLength/>
    <TimeStamp>2015-08-31T10:56:54-05:00</TimeStamp>
    <SenderID>36600582162711001</SenderID>
    <ReceiverID>37-1320188</ReceiverID>
    <CORERuleVersion>2.2.0</CORERuleVersion>
    <CheckSum/>
    <Payload> 999999999|10102023|10172023| </Payload>
  </cor:COREEnvelopeBatchSubmission>
```

Note the Request Payload is always submitted as a FILE ATTACHMENT. The FILE ATTACHMENT should be formatted in a fixed-sequence and pipe delimited ("|") (each field should be terminated with a pipe) and the sequence is as follows:

 <PayeeID>|<BeginDate>|<EndDate>|<Voucher Number>|<VoucherType>|<DownloadScopeIndicator>|.

If a field is to be {empty} and have no value, just the pipe delimiter terminating the field is required. For example, a payload request with just Payee ID and Voucher Number would be formatted 999999999|||777777777777|||. A payload request with Payee ID, Begin Date and End Date would be formatted 999999999|08/01/2024|08/30/2024||||. Note the pipe terminator for the Voucher Number field is still given to denote the Voucher Number field does not have a value.

Request Payload Code Set:

DESCRIPTION	VALID VALUES
Payee ID	Valid Payee ID number is always required
Voucher Number	{empty} or a valid voucher number (if a voucher number is supplied, the web service only uses the payee id and voucher number to locate the 835 file, all other request payload data fields are ignored)
Begin Date	{empty} or Required when no voucher number supplied or Required when an end date is supplied and Must be a valid date value prior to the end date's value
End Date	{empty} or Required when no voucher number supplied or Required when a begin date is supplied and Must be a valid date value older than the begin date value and Not be more than 31 calendar days from the begin date
Voucher Number	{empty} or If a voucher number is given, the search criteria fields (begin date, end date, voucher type, download scope indicator) are ignored and the payee's 835 file is returned
Voucher Type	{empty} or "I" for Institutional, "P" for Non-Institutional/Professional, or "D" for Drug/Pharmacy, or

	"A" for all voucher types
Download Scope Indicator	{empty} or "O" for only old files downloaded already in the past, or "N" for only new files which have never been downloaded yet, or "A" for all files, both old and new

Upon receipt of the SOAP request, the web service will verify the username and password submitted as valid/authorized to use the web service. If not authorized/valid, an error code and error message are returned. If valid/authorized, the web service will next analyze the request payload field values. The Payee ID is always required. If a Payee ID and Voucher Number are submitted, the web service will verify the username has authorization to the Payee ID's 835 files using MEDI's authorization records. If authorized, the web service searches for the specific voucher number. If found, the 835 file is returned in the batch response payload in a zipped format. If not authorized by the Payee or if the voucher number is not found, an error code and error message are returned. It should be noted, the only time the web service returns an 835 file is when the request contains the Payee ID and a specific Voucher Number. If the request does not contain a valid combination of Payee ID and Voucher Number, the web service instead returns a list of Voucher Numbers which meet the request payload search criteria. Depending on the search criteria submitted in the request payload, that list of Voucher Numbers could result in none, one, or greater than one voucher(s) found. Whatever voucher numbers are found meeting the criteria, that list of voucher numbers is returned in the response payload. Once the trading partner has received the list of voucher numbers, that list of voucher numbers can immediately be used to connect to the web service again to download each voucher number's 835 file, one voucher number at a time. The Payee ID must be supplied each time too.

Again, if the request payload does NOT contain a specific Voucher Number for the Payee ID (the Voucher Number field is {empty} / not populated with a value), the web service will perform a search for 835 files which meet the search criteria supplied within the request payload. The web service will search for vouchers for the supplied Payee ID which fall within the specified Begin Date and End Date, the specified Voucher Type ("I" for Institutional, "P" for Non-Institutional/Professional, or "D" for Drug/Pharmacy, or "A" for all voucher types), and the Download Scope Indicator ("O" for only old files which have been downloaded already in the past, or "N" for only new files which have never been downloaded yet, or "A" for all files both old and new). If the Voucher Type is {empty}/not specified, the web service will default to "A" and return voucher numbers for all voucher types found. Likewise, if the DSI is {empty}/not specified, the web service will default to New and return only voucher numbers that have never been downloaded yet. The list of voucher numbers found within SOI-HFS' IEC FTP Audit database meeting the request criteria specified in the request payload will be returned in the response payload. As stated above, that list of voucher numbers may be immediately used to perform 835 file download requests by specific Payee ID and Voucher Number.

Please note: a date range no more than 31 calendar-days range is permitted.

2) Sample 835 SOAP Request and Response:

```
<soap:Envelope xmlns:cor="http://www.caqh.org/SOAP/WSDL/CORERule2.2.0.xsd"
xmlns:soap="http://www.w3.org/2003/05/soap-envelope">
  <soap:Header><wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-
utility-1.0.xsd"><wsse:UsernameToken wsu:Id="UsernameToken-
A1685AE5C1C8CDB231173368143463752"><wsse:Username>P835TEST</wsse:Username><wsse:Password
Type="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-username-token-profile-
1.0#PasswordText">P835TEST1</wsse:Password><wsse:Nonce EncodingType="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-soap-message-security-
1.0#Base64Binary">yvj8LIzmorGY4c1v+op0FQ==</wsse:Nonce><wsu:Created>2024-12-
08T18:10:34.637Z</wsu:Created></wsse:UsernameToken></wsse:Security></soap:Header>
  <soap:Body>
    <cor:COREEnvelopeBatchResultsRetrievalRequest>
```

```
            <PayloadType>X12_835_Request_005010X221A1</PayloadType>
            <ProcessingMode>Batch</ProcessingMode>
            <PayloadID>835_TEST_1</PayloadID>
            <!--Optional:-->
            <PayloadLength>47</PayloadLength>
            <TimeStamp>2024-12-08T12:10:11-06:00</TimeStamp>
            <SenderID>XXXXXXX001</SenderID>
            <ReceiverID>37-1320188</ReceiverID>
            <CORERuleVersion>2.2.0</CORERuleVersion>
            <!--Optional:-->
            <CheckSum>3f8d8d3bae6089844320cb0ea716c3390e514fa2</CheckSum>
            <Payload><inc:Include href="cid:835_TEST_VoucherNum.txt"
xmlns:inc="http://www.w3.org/2004/08/xop/include"/></Payload>
        </cor:COREEnvelopeBatchResultsRetrievalRequest>
    </soap:Body>
</soap:Envelope>


<soapenv:Envelope xmlns:soapenv="http://www.w3.org/2003/05/soap-envelope">
    <soapenv:Body>
        <ns2:COREEnvelopeBatchResultsRetrievalResponse
xmlns:ns2="http://www.caqh.org/SOAP/WSDL/CORERule2.2.0.xsd">
            <PayloadType>X12_835_Response_005010X221A1</PayloadType>
            <PayloadID>835_TEST_1</PayloadID>
            <TimeStamp>2024-12-08T11:28:39-06:00</TimeStamp>
            <SenderID>37-1320188</SenderID>
            <ReceiverID>12312311231web001</ReceiverID>
            <CORERuleVersion>2.2.0</CORERuleVersion>
```

```
<Payload>UEsDBBQACAAIAClUb1kAAAAAAAAAAAAAAAAbAAAARmlsZTgzNV8yMDIzMzQ1RDAzM19hcmNoNoa
XZlXVLLbtswEPwV9bqqAAD70IHOjKcpiQVEKKRtKbm1qNEaNoEB75rd3LQm1kD0IIjEznN1ZGxUQAtn/+nR6fQVe5
5QzQoUwQW1XJaWkJkQ2oyKkAsYpowyILCV8QYWSUPxiVZTiH4zwlI4RunEnBkXFGUUgIzt6yQUBCvMqQmbG
qKIpTiB4eZek6TAG6FBTgx887GrToWkKHiWKWtxveFE2hHOgvN4eTs3UQ0HKB8FTQFHrnPWDjVlvGquVbZLniK
FZHE5Tlx2D8k2mzsafTGZUnJIvlI7B+mNrjWuQDxWrK764HE0APUPXxuz79Xa7fvzM3i+33z8uf37BZIDmoq5zdJiX
ZVUu6INb0H8vb+8f17dvt894QnJeVcirxGLYQH/ycTJh8+uyYKJRQXdZO5x8A6195HRvRWirvdIqTN0pZAd3bu4db
CJg/RpICqaF8fIB3WJKKbgYcbcRJlkzUVJQFBbPNkFMceC1Z0m4EWxe5FFLK9Q6jgl4vQM4lY0zWRBTkTsbJ9xSe
NQLPyjnzdYDWBI9zHu6B9gGwY3xJFmRBCgYMxs66g/UZEl6W3Od5Z2kJl3G2vEcE5SmeNXT6SUomitXPugD1
DqNVBD2AWptwz9AZ8EyQFLHDYt27l/pFx9Yo2C13+gdQSwcIHAZ7QuUBAABBAwAAUEsBAhQAFAAIAAgAKV
RvWRwGe0LIAQAAQQMAABsAAAAAAAAAAAAAAAAAAAAAAAEZpbGU4MzVfMjAyMzM0NUQwMzNfYXJjaGl2Z
VBLBQYAAAAAAQABAEkAAAAuAgAAAA=</Payload>
```

```
            <ErrorCode>Success</ErrorCode>
            <ErrorMessage>Envelope was processed successfully.</ErrorMessage>
        </ns2:COREEnvelopeBatchResultsRetrievalResponse>
    </soapenv:Body>
</soapenv:Envelope>
```

Request Payload Format: payload is an attached txt file in the SOAP request with "|" delimiter.
PAYEE NUMBER|BEGIN DATE|END DATE|VOUCHER NUMBER|VOUCHER TYPE|DOWNLOAD SCOPE INDICATOR

PAYEE NUMBER - HFS PAYEE NUMBER
BEGIN DATE - FORMAT YYYY-MM-DD
END DATE   - FORMAT YYYY-MM-DD
VOUCHER NUMBER -
VOUCHER TYPE - OPTIONAL, VALID VALUES ARE I,P,D
DOWNLOAD SCOPE INDICATOR- OPTIONAL VALID VALUES ARE O, N, A

If voucher number not provided, webservice will return voucher number in a text file.
Sample:
vouchernumber1
vouchernumber2
vouchernumber3
... and so on

If a Voucher number is provided in the request payload, the webservice will return the 835 file.

4.3   Transmission Administrative Procedures

4.3.1   Structure Requirements

There is a constraint on 835 message size of 10 MB. It is strongly encouraged that submitters retrieve 835's frequently, as per their respective payment cycles.

4.4   Re-Transmission Procedures

If the HTTP post reply message is not received within the 90-second response period, the user's CORE compliant system should send a duplicate transaction no sooner than 90 seconds after the initial attempt was sent.

If no response is received after the second attempt, the user's CORE compliant system should submit no more than one duplicate transaction within the next 30 minutes. If the additional attempt results in the same timeout termination, the user's CORE compliant system should notify the user to contact SOI-HFS or the information source directly to determine if system availability problems exist or if there are known internet traffic constraints causing the delay.

4.5   4.5 Communication Protocols

4.5.1   SOAP + WSDL

SOI-HFS also supports transactions formatted according to the Simple Object Access Protocol (SOAP) conforming to standards set forth by the Web Services Description Language (WSDL) for XML envelope formatting, submission, and retrieval.

4.5.1.1   *SOAP XML Schema*

The XML schema definition set forth by CORE is located at:
http://www.cagh.oraISOAPIWSDUCORERule2.2.0.xsd

4.5.1.2   *WSDL Information*

The WDSL definition set forth by CORE is located at:
http://www.cagh.org/SOAPIWSDUCORERule2.2.0.wsdl

4.5.1.3   *SOAP Version Requirements*

SOI-HFS requires that all SOAP transactions conform to SOAP Version 1.2.

4.5.2   Header Requirements

Field	Accepted Values	Comment
PayloadType	X12_835_Request_005010X221A1	Batch Submissions
	X12_005010_Response_005010X221A1	Batch Results Retrieval
ProcessingMode	Batch	Batch used for either submission or pickup
TimeStamp	YYYY-MM-DDTHH:MM:SSZ	See http://www.w3.org/TR/xmlschm11-2/#dateTime
SenderID	SOI-HFS Assigned EDI Submitter ID	
ReceiverID	37-1320188	
CORERuleVersion	2.2.0	

4.5.3   Error Reporting

HTTP	Errors associated with connectivity, authorization, etc. will be reported at this level
HTTP 200 OK	No errors
HTTP 202 Accepted	Batch submission accepted
HTTP 400 Bad Request	Error with HTTP header
HTTP 403	Authentication failed
HTTP 500 Internal Server Error	Unexpected error during processing

Envelope	Errors regarding the structure of data included within the body of the message will be reported at this level in a response of type form-data.
Success	No errors
PayloadTypeRequired	Missing PayloadType
PayloadTypeIllegal	Invalid or unsupported PayloadType
ProcessingModeRequired	Missing ProcessingMode
ProcessingModeIllegal	Invalid or unsupported ProcessingMode
SenderIdRequired	Missing SenderId
SenderIdIllegal	Invalid SenderId

ReceiverIdRequired	Missing ReceiverId
ReceiverIdIllegal	Invalid ReceiverId

5 CONTACT INFORMATION

5.1 EDI CUSTOMER SERVICE and TECHNICAL ASSISTANCE

If you have problems with the web service, use the following contact information to contact HFS:

SOI Dept. of Innovation & Technology (DoIT) Service Desk at 1-312-814-DoIT (3648),
Option #1 - for Information Technology (IT), and then Option #2 - for SOI-HFS

Or send HFS an e-mail: hfswebmaster@illinois.gov

When contacting for assistance, have the following information ready for the most efficient service:
- The name, HFS provider number, and/or NPI of the provider on whose behalf you are calling.
- A detailed description of your issue. Include any error messages that you receive. If you know in which loop and/or segment the issue is occurring, please provide that information as well.
- Your SOI-HFS assigned submitter ID/user ID.
- Any related reports that you may have received from SOI-HFS.
- If you are calling regarding claims, have the specific information on the claim(s) in question (recipient ID, recipient name, date of service, amount). If it involves a large number of claims, let us know how many claims are affected and have two or three example claims for the technician to check.
- If you are calling regarding remittances, have the specific information on the payment (voucher number, voucher date, voucher amount, line of business, and the payee ID number).
- For eligibility, claim status, and other requests, the time when the request was sent and the result.
- Leave a contact number or e-mail address at which an SOI-HFS EDI Support representative can reach you when returning your communication.

5.2 PROVIDER SERVICE NUMBER

For issues not directly related to EDI (e.g. adjudication issues for claims), contact a Billing Consultant at 1-877-782-5565 or for issues pertaining to Long Term Care, contact the Bureau of Long Term Care at 1-844-528-8444.

5.3 APPLICABLE WEBSITES/E-MAIL

More information on the EDI submission process can be found at the following web page:
https://hfs.illinois.gov/medicalproviders/edi/medi.html

The MEDI FAQ may be a useful resource:
https://hfs.illinois.gov/medicalproviders/edi/medi/faqs.html

The MEDI Manual may be downloaded:
https://hfs.illinois.gov/content/dam/soi/en/web/hfs/medicalproviders/edi/medi/medihelp/medimanual.pdf

All SOI-HFS X12 HIPAA Transaction Companion Guides can be found at:

https://hfs.illinois.gov/medicalproviders/handbooks/5010.html

Information pertaining to EDI Control can be found at:
https://hfs.illinois.gov/content/dam/soi/en/web/hfs/sitecollectiondocuments/061711edic.pdf

6 CONTROL SEGMENTS/ENVELOPES

6.1 ISA-IEA

This section describes SOI-HFS' use of the interchange control segments. It includes a description of expected sender and receiver codes, authorization information, and delimiters.

The values required within the payload transaction's Interchange Control Header (both Inbound to SOI-HFS and outbound from SOI-HFS) can be found within SOI-HFS' downloadable PDF ASC X12 Implementation Guide version 005010X221and the ERRATA 005010X221A1 dated June 2010 at:
https://hfs.illinois.gov/content/dam/soi/en/web/hfs/sitecollectiondocuments/835.pdf.

6.2 GS-GE

This section describes SOI-HFS' use of the functional group control segments. It includes a description of expected application sender and receiver codes. Also included in this section is a description concerning how SOI-HFS expects functional groups to be sent and how State of Illinois Healthcare and Family Services will send functional groups. These discussions will describe how similar transaction sets will be packaged and SOI-HFS' use of functional group control numbers.

The values required within the payload transaction's Interchange Control Header (both Inbound to SOI-HFS and outbound from SOI-HFS) can be found within SOI-HFS' downloadable PDF ASC X12 Implementation Guide version 005010X221and the ERRATA 005010X221A1 dated June 2010 at:
https://hfs.illinois.gov/content/dam/soi/en/web/hfs/sitecollectiondocuments/835.pdf.

6.3 ST-SE

Each 835 request within a batch transaction must be wrapped in its own ST-SE segment. For batch transactions, only the first ST-SE grouping in the first batch request will be processed and given a response. Real time 835 transactions are not supported.

7 PAYER SPECIFIC BUSINESS RULES AND LIMITATIONS

Daily Claims Adjudication and Remittance Advice Cycle

There are variations/exceptions to the rule, but majority of the time the SOI mainframe platform adjudicates claims for payment on a nightly batch business cycle (business days only, not holidays nor weekends). Each mainframe business cycle produces a voucher file which contains one voucher record per Payee. Each voucher record represents a payment for all claims adjudicated (all claims received from all providers associated with the Payee) since the previous successful execution of the batch cycle. In summary, each record in the voucher file represents one payment per Payee which is payment for all associated provider claims adjudicated in the current mainframe batch cycle.

At the end of the mainframe batch cycle, the voucher file is FTP to an internal staging server/environment for further distribution processing. Within this environment, dedicated maps execute to split the voucher file into many files, one X12 835 electronic remittance advice (ERA) file per Payee. Each of the 835 ERA files are placed into a pending payment status, unless there is no payment (a voucher which has a zero dollar payment amount). If the payment is a zero-dollar amount, the X12 835 ERA file is immediately finalized and routed to the MEDI/IEC FTP Audit database where it becomes available for download to the external trading partners via two EDI connection options: 1) MEDI's Internet Electronic Claims (IEC) ERA Download web page, and/or 2) the Agency's CAQH CORE Web Service. Both connections require prior registration/authorization before they can be utilized. However, if the voucher payment amount is greater than zero for the 835 ERA file, the file remains in pending status and a voucher is sent to the Comptroller for payment processing. After the Comptroller completes payment, the Comptroller returns a Warrant file to SOI-HFS containing the payment information for each voucher. This

payment data gets routed to the staging server/environment to update the pending 835 ERA files with the corresponding payment data. After each 835 ERA file has been updated with its payment data, it is immediately finalized and routed to the IEC FTP Audit database where it becomes available for download to the external trading partners (Payees) via the same two EDI avenues described above.

835 File Composition

Each X12 835 ERA file contains adjudication information for the current batch cycle for one voucher, one payee, many providers, one or more claims per provider, and one or more service lines per claim. The batch cycle's timeframe (the contents of the X12 835 ERA file) could be just one day's processing or potentially more than one day. It depends on the adjudication cycle and there are many factors that can interrupt the daily cycle to become more than one day's worth of claims. Regardless, all claims adjudicated since that last successful voucher cycle for a given payee (and the providers for which they receive payment) are included in the current cycle's voucher file (X12 835 ERA file).

835 File Download Process

When a trading partner downloads X12 835 ERA file(s) (no matter which connection avenue they utilize, MEDI/IEC or the CAQH CORE web service), each X12 835 ERA file(s) downloaded has a downloaded-flag turned on in the file's corresponding record in the IEC FTP Audit database as having been downloaded. Files that have been downloaded in the past (those with this downloaded-flag turned on in the database record representing the 835 file) will not be included in searches for new 835 vouchers. The default action by the web service is to return only voucher numbers for files that have never been downloaded in the past (only files for which the downloaded-flag is turned off). 835 ERA files remain available for downloading again for a period of one year from the date the file became available for download.

Trading partners can control whether older files that have already been downloaded in the past are included in the response through the use of the DOWNLOAD-SCOPE-IND field located in the request payload format. The DOWNLOAD-SCOPE-IND field's code set values are "N" (return only **New** voucher numbers meeting the request criteria), "O" (return only **Old** voucher numbers meeting the request criteria), or "A" (return **All**, both new and old, voucher numbers meeting the request criteria). If no value is given in the DOWNLOAD-SCOPE-IND field in the request payload, <u>the default action will be to return only New voucher numbers in the response</u>. This is discussed in more detail in a prior section (4.2 Process Flows) in this document.

8 ACKNOWLEDGEMENTS AND/OR REPORTS

SOI-HFS currently DOES NOT receive Acknowledgement files for 835 transactions exchanged via the CORE web service.

9 TRADING PARTNER AGREEMENTS
9.1 TRADING PARTNERS

An EDI Trading Partner is defined as any SOI-HFS trading partner (provider, physician, pharmacy, pharmacist, billing service, clearinghouse, payee [financial institution], other business, etc.) that exchanges (transmits to or receives from) electronic data interchanges with SOI-HFS.

Payers have EDI Trading Partner Agreements to ensure the integrity of the electronic transaction process. The Trading Partner Agreement is related to the electronic exchange of information, whether the agreement is an entity or a part of a larger agreement, between each party to the agreement.

For example, a Trading Partner Agreement may specify among other things, the roles and responsibilities of each party to the agreement in conducting standard transactions.

10 TRANSACTION SPECIFIC INFORMATION

This section describes how ASC X12N Implementation Guides (IGs) adopted under HIPAA will be detailed with the use of a table. The tables contain a row for each segment that SOI-HFS has something additional, over and above, the information in the IGs. That information can:

- Limit the repeat of loops, or segments
- Limit the length of a simple data element
- Specify a sub-set of the IGs internal code listings
- Clarify the use of loops, segments, composite and simple data elements
- Any other information tied directly to a loop, segment, composite or simple data element pertinent to trading electronically with SOI-HFS

In addition to the row for each segment, one or more additional rows are used to describe SOI-HFS' usage for composite and simple data elements and for any other information. Notes and comments should be placed at the deepest level of detail. For example, a note about a code value should be placed on a row specifically for that code value, not in a general note about the segment.

The following table specifies the columns and suggested use of the rows for the detailed description of the transaction set companion guides.

Page #	Loop ID	Reference	Name	Codes	Length	Notes/Comments
193	2100C	NM1	Subscriber Name			This type of row always exists to indicate that a new segment has begun. It is always shaded at 10% and notes or comment about the segment itself goes in this cell.
195	2100C	NM109	Subscriber Primary Identifier		15	This type of row exists to limit the length of the specified data element.
196	2100C	REF	Subscriber Additional Identification			
197	2100C	REF01	Reference Identification Qualifier	18, 49, 6P, HJ, N6		These are the only codes transmitted by Acme Health Plan.
			Plan Network Identification Number	N6		This type of row exists when a note for a particular code value is required. For example, this note may say that value N6 is the default. Not populating the first 3 columns makes it clear that the code value belongs to the row immediately above it
218	2110C	EB	Subscriber Eligibility or Benefit Information			
231	2110C	EB13-1	Product/Service ID Qualifier	AD		This row illustrates how to indicate a component data element in the Reference column and also how to specify that only one code value is applicable.

A. APPENDICES

1. Implementation Checklist

This appendix contains all necessary steps to achieve the purpose of this document.

1) Acquire a SOI Digital ID (username and password) for access to MEDI.
2) Log into MEDI and establish a new account or become an admin or employee of an existing account.
3) Establish all necessary payee authorizations required to be able to download 835 ERA files.
4) Complete a SOI-HFS Trading Partner Application and Trading Partner Agreement.
5) Register your CAQH CORE username and password within MEDI to have authorized connectivity to the CAQH CORE web service.
6) Download the WSDL files needed to connect/consume the SOI-HFS CAQH CORE web service.

2. Frequently Asked Questions

What information should I have immediately available when I contact SOI-HFS with an issue with the CAQH CORE web service?

When calling EDI Support as a vendor or clearinghouse, have the following information ready for the most efficient service:

- The name, HFS provider number, and/or NPI of the provider on whose behalf you are calling.
- A detailed description of your issue. Include any error messages that you receive. If you know in which loop and/or segment the issue is occurring, please provide that information as well.
- Your SOI-HFS assigned submitter ID/user ID.
- Any related reports that you may have received from SOI-HFS
- If you are calling regarding claims, have the specific information on the claim(s) in question (recipient ID, recipient name, date of service, amount). If it involves a large number of claims, let us know how many claims are affected and have two or three example claims for the technician to check.
- If you are calling regarding remittances, have the specific information on the payment (voucher number, voucher date, voucher amount, line of business, and the payee ID number).
- For eligibility, claim status, and other requests, the time when the request was sent and the result.
- Leave a contact number or e-mail address at which an SOI-HFS EDI Support representative can reach you when returning your communication.

3. Change Summary

This section describes the differences between the current version Companion Guide and previous version.

Change#	Chapter and Section	Change Description	Date of Change	Version
1			10/12/2024	
2				
3				