

270/271 Enhanced Eligibility Initiative Real Time Transaction Connectivity Specifications and Supporting Documents

The MN HIPAA Collaborative members, and other participating organizations, have agreed to endorse the recommendations for the “Enhanced Eligibility” search criteria, transaction data content, and the connectivity protocol HTTPS for Real Time processing of the 270/271 transaction. The purpose of this document is to define the various parameters around using HTTPS (HTTP over SSL) on the public Internet to connect directly to participating payer systems for transmission and receipt of the ANSI ASC X12N 270/271 Eligibility Inquiry and Response transaction.

This document is intended for the use of provider information systems departments, practice management or hospital information system vendors, and clearinghouses that provided eligibility verification services.

Payers Supporting This Connection Method

- Blue Cross Blue Shield of Minnesota (an independent licensee of the Blue Cross and Blue Shield Association)
- HealthPartners
- Medica
- Minnesota Department of Human Services
- PreferredOne
- UCare Minnesota

Guiding Principles

The Minnesota HIPAA Collaborative’s intention is to:

- Support the use of connectivity standards that will incur little or no cost to trading partners.
- The protocols must be readily available and supported by most hardware/software vendors or available on the Internet, and they should be widely accepted and used across the industry.
- Be supported by all payers and minimize the “customization” needed for direct connection to each payer.
- Offer the ability to connect to all participating payers directly in a similar or identical way.
- Provide a method for supporting the HIPAA transaction standard for system-to-system EDI that does not include a web browser, forms-based inquiry and response process, but is truly machine-to-machine exchange of the transaction.
- This defined method of connection is not exclusive. Participating payers may offer other options for direct connection to perform Real Time 270/271 transactions. You should contact each payer directly to determine other available options.

General Description of the Connection Method

- A detailed definition of HTTPS and how to use it can be found at www.silurian.com/sitevigil/HTTPS.htm
- The encryption method supported by all participating payers is Secure Sockets Layer (SSL) over the public Internet. If you are using TLS, there may be issues of interoperability. Please contact the respective payer to determine if the use of TLS is compatible with their environment.
- Each payer's production ready time frame to support this specific method of connection varies. Depending on the payer you wish to connect to, please contact them directly to determine their target implementation date.
- This HTTPS connection method is designed for use in a traditional EDI (machine-to-machine) process. It is not intended to accommodate individual user-specific login and browser-based use. Browser-based systems may also be available depending on each payer's respective capabilities.
- This Real Time 270/271 transaction process is designed for single patient/member inquiries only. It is not designed to support Batch 270/271 and it is not intended to support large quantities, or "bursts" of single inquiry transactions from a single source. Capacity and response time may vary by payer, as their internal system environments will differ.

Security and Authentication Requirements

- All Collaborative members will use ID and Password as the default authentication requirements. Participating payers have agreed to support ID & Password authentication as a minimum criteria (e.g. no individual 3rd party certificates will be required beyond the normal ubiquitous SSL Internet certification process).
- User ID and Password authentication is based on a scripted process to be contained in the header of the HTTP Post Message, and not through a forms-based authentication model.
- Issuance, maintenance and control of Password requirements may vary by trading partner. You should contact each trading partner to determine their ID and Password policies and requirements.
- Providers or clearinghouses should contact each payer directly to obtain an appropriate ID and Password.
- Some trading partners may require additional security for file transmissions, such as the use of Gnu Privacy Guard (GPG), or PGP for additional encryption. Please contact each trading partner directly to determine if such additional encryption is required for this transaction.

Response Time, Time Out Parameters and Re-Transmission

- The ASC X12N 004010X092A1 Implementation Guide recommends a 60 second or less response time for the Real Time implementation of this transaction. All participating payers will attempt to generate a response to a Real Time 270 Eligibility Inquiry transaction within the 60 second time frame, and optimally far less than 60 seconds. Participating payers understand the time sensitive nature and the business process needs of the provider community, and will attempt to respond to Real Time 270's received in the least amount of time possible. Actual response time may vary from payer to payer.
- There may be circumstances under which a corresponding 271 Eligibility Response transaction may take longer than the recommended 60 seconds. Therefore, we suggest that submitting providers or clearinghouses using this Real Time synchronous process configure a time-out parameter for the reply

to the HTTP Post Message sent. Because the actual routing and processing of a Real Time 270/271 could exceed 90 seconds in some instances, due to transaction routing and 3rd party response issues, we recommend a minimum time-out setting of 120 seconds before the submitter's system would terminate the original message.

- In the event that an HTTP Post Reply Message is not received within the maximum 120 second response period, we recommend provider or clearinghouse submitters send a duplicate 270 transaction no sooner than 5 minutes after the original attempt.
- If no response is received after the second attempt, we recommend providers or clearinghouses submit no more than 5 duplicate 270 transactions. If the additional attempts result in the same time-out termination, we suggest the submitter contact the payer by phone to determine if system availability problems exist, or if there are known Internet traffic constraints which are causing the delay.

Response Message Options and Error Notification

- The HTTP Post Message process requires a response (or “reply”) to the message that was sent. The response sent back from the message receiver (e.g. the various payers) can fall into several different categories. The possible response messages/transactions could be one of the following:
 1. A standard HTTP error message, especially error codes 500 and 503. This type of response would generally indicate there was some problem with the Internet, or a failure during the authentication process or connection to the payer's system. To find out more about standard HTTP error messages and their interpretation, go to (<ftp://ftp.isi.edu/in-notes/rfc2616.txt>). See Section 10: Status Code Definitions.
 2. A negative 997 could be received if the submitted 270 transaction failed syntax compliance validation. **It is strongly recommended that no positive 997 or TAI should be requested by the submitting trading partner using this Real Time transaction method.** Returning these receipt acknowledgement transactions would terminate the HTTP Post Message prematurely.
 3. Payers may return a 271 to communicate to the submitter that semantic compliance failure has occurred. Each payer will have their documented use of the 271 for semantic error notification on their respective web sites, or through their EDI support departments. The level of compliance validation for 270 transactions may vary by payer, therefore you should contact each payer to determine their compliance validation requirements.
 4. The optimum reply transaction is the 271 Eligibility Response. Participating payers have agreed to a common set of search criteria (see “[270/271 Search Parameters](#)” – **make a doc link on the Collab web site**) and eligibility and benefit information (see “[MN HIPAA Collaborative Enhanced Eligibility Companion Document](#)” (**make a doc link on the Collab web site**)). These documents can also be found on the MN HIPAA Collaborative web site. If processing errors occur, the 271 will contain AAA segments with standard code values describing the reason for failure. Please see the ASC X12N 004010X092A1 Implementation Guide for details.

What is Needed to Set Up This Method of Connection

- Access to the public Internet.
- Communication software or web server that supports HTTP version 1.1 (or higher) and SSL.
- You will need to provide this document to your information systems department, your practice management system or hospital system vendor, or your clearinghouse as they will need to create or modify an applications software program to support this connection method.

- This Real Time 270/271 is designed for single inquiries only using the HIPAA standard transaction in true EDI mode (machine-to-machine). It is not intended to support web browser-driven inquiries or screen-scraping utilities.

Example of Creating an HTTP Post Message Header

- Below is an example Java script language and resultant HTTP Post Message Header which shows how to script the ID and Password in the HTTP Post Message.

Sample code to populate the basic authentication header fields when generating an HTTP Post Message

(example shown is Java code to create HTTP code to create the HTTP Post Header).

```
System.Net.WebRequest request = base.GetWebRequest(uri);
string username = "Fflinstone";
string password = "I_love_Wilma";
string auth = username + ":" + password;
byte[] binaryData = new Byte[auth.Length];
binaryData = Encoding.UTF8.GetBytes(auth);
auth = Convert.ToBase64String(binaryData);
auth = "Basic " + auth; request.Headers["AUTHORIZATION"] = auth;
return request;
```

You will get a header that looks like:

```
<HTTPHeaders>
<user-agent>Mozilla/4.0 (compatible; MSIE 6.0; MS Web Services Client Protocol 1.1.4322.2032)</user-agent>
<authorization>Basic RkZsaW5zdG9uZTpJX2xvdmVfV2lsbWE=</authorization>
<content-type>text/xml; charset=utf-8</content-type>
<soapaction>" "</soapaction>
<content-length>930</content-length>
<expect>100-continue</expect>
<connection>Keep-Alive</connection>
<host >localhost:8080</host>
</HTTPHeaders>
```