

BACKGROUND

This rule addresses proposed usage patterns for both batch and real time transactions, the exchange of security identifiers, and communications-level errors and acknowledgements. It does not attempt to define the specific content of the message exchanges beyond declaring that the HIPAA-mandated X12 formats must be used between covered entities and security information must be sent outside of the X12 payload.

This rule is designed to provide a “safe harbor” that application vendors, providers, and health plans (or other information sources) can be assured will be supported by any CORE-certified trading partner. All CORE-certified organizations must demonstrate the ability to implement connectivity as described in this rule. This rule is not intended to require trading partners to remove existing connections that do not match the rule, nor is it intended to require that all CORE trading partners must use this method for all new connections. CORE expects that in some technical circumstances, trading partners may agree to use different communication mechanism(s) and/or security requirements than that described by this rule.

This rule describes some of the specifics for implementing HTTP/S connectivity for healthcare administrative transaction exchange.

RULE

CORE-certified entities must be able to implement HTTP/S Version 1.1 over the public Internet as a transport method for the eligibility inquiry and response transactions (270/271). Information Sources must be able to perform the role of an HTTP/S server, while Information Receivers must be able to perform the role of an HTTP/S client. HTTP/S is a secure, reliable, ubiquitous protocol that has a proven record of support for high-volume transaction exchange and security in healthcare and other industries. In addition, there is wide system-developer and software tools support for HTTP/S, making it a relatively inexpensive transport for information sources and receivers to support.

Section 1: Usage Patterns

HTTP/S supports a request-response message pattern, meaning that the sender submits a message and then waits for a response from the message receiver. This works well for the submission of both batch and real time X12 messages, but the response message from the receiver is different depending on whether the sender’s message is a real time request, batch submission, or batch request pickup.

Section 2: Real Time Requests

Real time requests must include a single inquiry or submission (e.g. one eligibility inquiry to one information source for one patient). In this model the response from the message receiver is either an error response (see below for error reporting) or the corresponding X12 message response (e.g. a TA1, 997 or 271 if the request was a 270).

Section 3: Batch Submission

Batch requests are sent in the same way as real time requests. In this model the response will differ because message receivers are not required to provide an X12 response in the timeframes specified by CORE for real time. For batch submissions, the response must be only the standard HTTP message indicating whether the request was accepted or rejected (see below for error reporting.) Message receivers must not respond to a batch submission with an X12 response such as a TA1 or 997 as described in the CORE 150: Eligibility and Benefits Batch Acknowledgement Rule version 1.0.0 in the HTTP response to the batch request, even if their systems’ capabilities

allow such a response. (See the CORE 155: Batch Response Time Rule version 1.0.0 for the response time requirements for TA1 or 997.)

For full details of the standard HTTP messages, see [RFC 2616](#).¹ In general a 2xx series response means that the batch submission has been accepted for further processing, while a 4xx or 5xx series response means that the submission has not been accepted and will not be processed by the message receiver.

Subsection 3.1: Batch Response Pickup

Batch responses should be picked up after the message receiver has had a chance to process a batch submission (see the CORE 155: Batch Response Time Rule version 1.0.0 for details on timing). Under this usage pattern, the message sender connects to the message receiver using HTTP/S and sends a message requesting available files, and responder then sends back either.

- 1) The file(s) in the HTTP/S response message (payload), or
- 2) A list of available file(s), and supports a mechanism to request a particular file from the list.

Section 4: HTTP Data Elements Required and Message Format

Subsection 4.1: Required Data Elements

Certain business data elements: authorization information, a payload identifier, and date and time stamps, must be included in the HTTP message body outside of the X12 data.

Information Sources must publish their detailed specification for the message format in their publicly available Companion Guide.

In order to comply with the CORE 155 and 156: Response Time Rules version 1.0.0, message receivers will be required to track the times of any received inbound messages, and respond with the outbound message for that payload ID. In addition, message senders must include the date and time the message was sent in the HTTP Message Header tags.

Subsection 4.2: Date and Time Requirements

This Phase I rule does not define the exact format and attributes for these data elements except that the date must be sent and logged using 8 digits (YYYYMMDD) and time must be sent and logged using a minimum of 6 digits (HHMMSS).

This Rule does not address issues of Batch Response Integrity; those are addressed by the CORE 150 Batch Acknowledgements Rules version 1.0.0.

Section 5: Security and Authentication Requirements

By using the HTTP/S protocol, all information exchanged between the sender and receiver is encrypted by a session-level private key negotiated at connection time. This approach makes it very difficult for an intruder to decode the encrypted data.

Subsection 5.1: User ID and Password

CORE participants will employ User ID and Password as the default minimum criteria authentication mechanism. Issuance, maintenance and control of password requirements may vary by participant and should be issued in accordance with the organizations' HIPAA Security Compliance policies. CORE recommends that the User ID and Password policies and requirements be published in each password issuer's Companion Guide.

¹The Internet Society. Network Work Group. <http://www.ietf.org/rfc/rfc2616.txt>. June 1999.

The User ID and Password authentication must be encrypted by the HTTP/S protocol, but passed outside of the X12 payload information as described in the HTTP Message format section. This allows message receivers to authenticate that the message is from a trusted source before passing it to their X12 parsing engine.

The receiver may also require the message sender to register the IP address for the host or subnet originating the transaction, and may refuse to process transactions whose source is not registered or does not correspond to the ID used.

Due to programming requirements of POSTing over HTTP/S, use of a digital certificate is required to establish communications. CORE-certified participants will make available information on how to obtain the receiver's root public certificate.

No additional security for file transmissions, such as the separate encryption of the X12 payload data, is required in this Phase I CORE Rule for connectivity. By mutual consent, organizations can implement additional encryption, but HTTP/S provides sufficient security to protect healthcare data as it travels the Internet.

Section 6: Response Time, Time Out Parameters and Re-transmission

This section of the rule relates to connectivity and telecommunications response times and time outs. The CORE 150 and 151 Batch and Real Time Acknowledgements Rules version 1.0.0. describe the responsibilities of CORE participants in responding to business messages (e.g. the X12 270) with the appropriate business response (e.g. the X12 TA1, 997, 271, etc).

If the HTTP Post Reply Message is not received within the 60 second response period, the provider's system should send a duplicate transaction no sooner than 90 seconds after the original attempt was sent.

If no response is received after the second attempt, the provider's system should submit no more than 5 duplicate transactions within the next 15 minutes.

If the additional attempts result in the same timeout termination, the provider's system should notify the provider to contact the health plan or information source directly to determine if system availability problems exist or if there are known Internet traffic constraints causing the delay.

Section 7: Response Message Options and Error Notification

This section of the rule addresses only the HTTP Post Message responses. Please refer to CORE 150 and 151 Eligibility and Benefits Acknowledgement Rules version 1.0.0 for required acknowledgments.

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 information sources) can fall into several different categories depending on the type of the request and the capabilities of the message receiver.

Subsection 7.1: Authorization Errors

If the username and/or password included in the request are not valid according to the message receiver, the message receiver must send back an HTTP 403 Forbidden error response with no data content.

Subsection 7.2: Batch Submission Acknowledgement

At the message acknowledgement level, a message receiver must send back a response with a status code of HTTP 202 Accepted once the message has been received. This does not imply that the X12 content has been validated or approved.

Subsection 7.3: Real Time Response or Response to Batch Response Pickup

When a message receiver is responding to a real time request or a batch response pickup request, assuming that the message authorization passed, the receiver must respond with an HTTP 200 Ok status code and the X12 data content as specified by the CORE 150 and 151 Batch and Real Time Acknowledgements Rules version 1.0.0.

Subsection 7.4: Server Errors

It is possible that the HTTP server is not able to process a real time or batch request. In this case, the message receiver must respond with a standard HTTP 5xx series error such as HTTP 500 Internal Server Error or HTTP 503 Service Unavailable. If a sender receives a response with this error code, they will need to resubmit the request at a later time, because this indicates that the message receiver will never process this message.

CONFORMANCE

Conformance with this connectivity rule is considered achieved by information sources if all of the following criteria are achieved:

- 1. The Information Source must publish their detailed HTTP Message format specification in a publicly available Companion Guide.*
- 2. The Information Source must demonstrate the ability to respond in their production environment to valid and invalid logon/connection requests with the appropriate HTTP errors as described in the Response Message Options & Error Notification section of this rule.*
- 3. The Information Source must demonstrate the ability to log, audit, track and report the required data elements as described in the HTTP Message Format section of this rule.*
- 4. The Information Source's HTTP/S-based connectivity method must be available for use by submitters for 95 percent of the information source's documented system availability as specified in the CORE System Availability rule and measured over a calendar month. Each CORE-certified entity must demonstrate its conformance with this criterion by demonstrating their ability to track and report the times the HTTP/S-based connectivity system was available.*

Conformance with this rule must be demonstrated through successful completion of the approved CORE test suite for this rule with a CORE-authorized testing vendor.