CAQH CORE

Phase IV CAQH CORE 470 Connectivity Rule v4.0.0

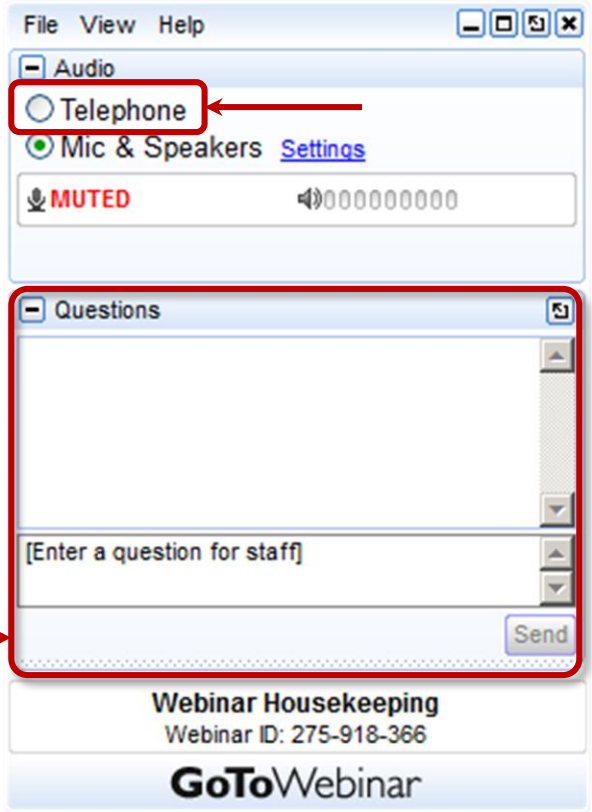
Drill Down on Requirements

Wednesday,
April 20th, 2016
2:00 – 3:00 PM ET

Logistics
How to Participate in Today's Session

- Download a copy of today's presentation on the CAQH.org website
  - Navigate to the CORE Education Events page and access a pdf version of today's presentation under the section for today's event
  - Also, a copy of the slides and the webinar recording will be emailed to all attendees in the next 1-2 business days
- The phones will be muted upon entry and during the presentation portion of the session
- At any time throughout the session, you may communicate a question via the web

Questions can be submitted ***at any time*** with the **Questions panel on the right side of the GoToWebinar desktop**



Session Outline

- Background & Evolution of the Connectivity Requirements
  - Safe Harbor Principle
- Phase IV CAQH CORE Connectivity Requirement Applicability
- Phase IV CAQH CORE 470 Connectivity Requirements
- Q&A/Commonly Asked Questions
- Appendix

Polling Question #1

Rate your understanding of the CORE Safe Harbor principle on a scale of 1-5.

1. Very Strong
2. Somewhat Strong
3. Neither strong nor weak
4. Somewhat Weak
5. Very Weak

Background & Evolution of the Connectivity Requirements & Safe Harbor Principle

Robert Bowman
Associate Director

ACA Mandated Operating Rules and Certification
Compliance Dates

Phases I-II COMPLIANCE	Phase III COMPLIANCE	ACA-Mandated HHS Health Plan Certification	Phase IV
January 1, 2013	January 1, 2014	TBD	Currently Voluntary
Health plan eligibility Claim status transactions *HIPAA covered entities conduct these transactions using the CAQH CORE Operating Rules*	Electronic funds transfer (EFT) Health care payment and remittance advice (ERA) *HIPAA covered entities conduct these transactions using the CAQH CORE Operating Rules*	ACA mandates health plans must certify to HHS compliance with Eligibility/ Claim Status/ EFT/ERA operating rules and underlying standards *Applies only to health plans and includes potential penalties for incomplete certification*	Health claims or equivalent encounter information Referral, certification and authorization Enrollment/ disenrollment in a health plan Health plan premium payments Health claims attachments (HHS Standard not yet mandated)
Mandated Requirements	Mandated Requirements	New HHS proposed rule TBD	Phase IV Op Rules approved for voluntary implementation by CAQH CORE Participating Orgs and CORE Board

Scope of Phase IV CAQH CORE Rule Requirements

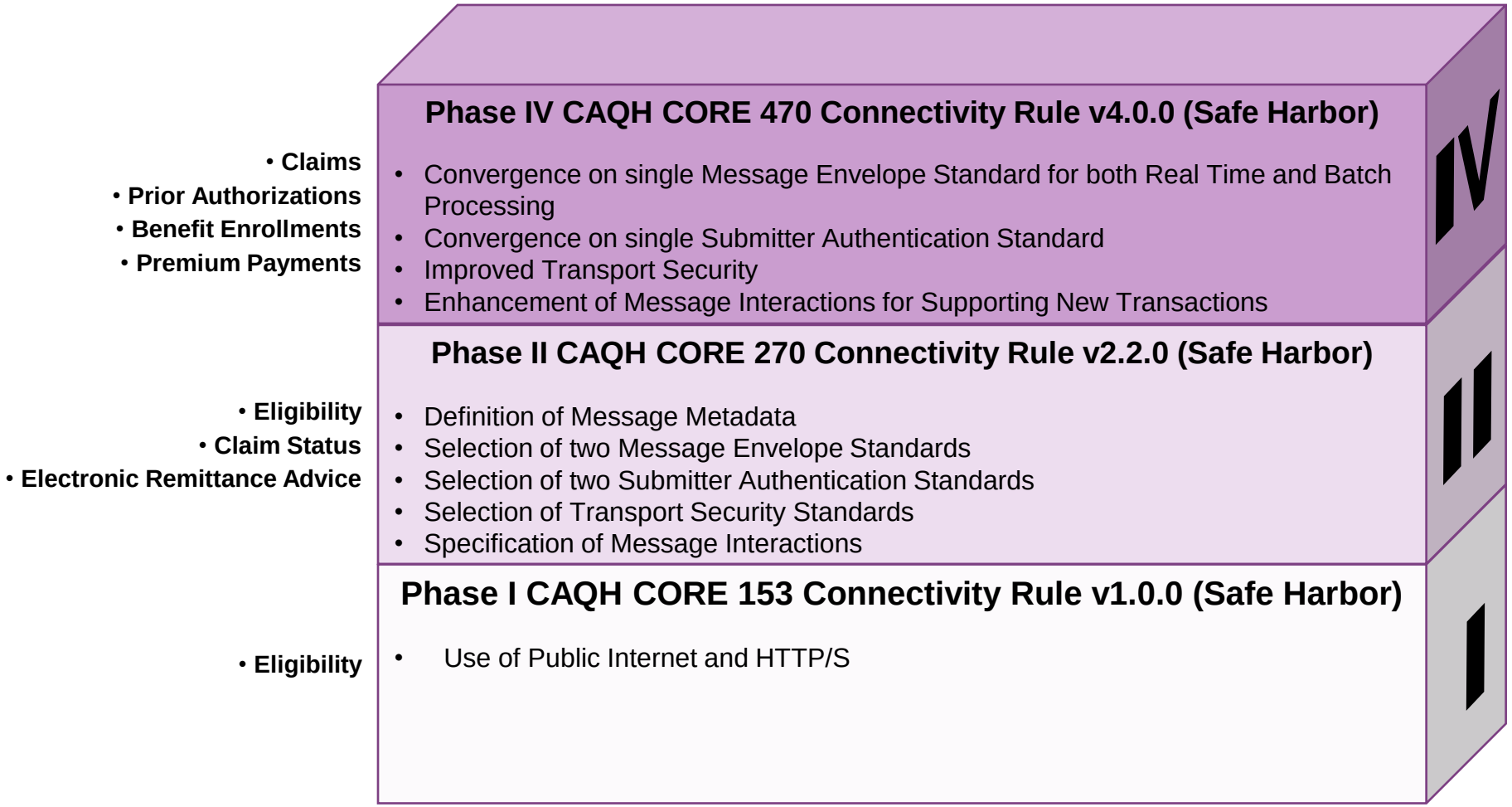
Infrastructure Requirement	Prior Authorization	Claims	Enrollment/ Disenrollment	Premium Payment
Processing Mode	*Batch OR Real Time Required*	*Batch Required; Real Time Optional*	*Batch Required; Real Time Optional*	*Batch Required; Real Time Optional*
Batch Processing Mode Response Time	*If Batch Offered*	**X**	**X**	**X**
Batch Acknowledgements	*If Batch Offered*	**X**	**X**	**X**
Real Time Processing Mode Response Time	*If Real Time Offered*	*If Real Time Offered*	*If Real Time Offered*	*If Real Time Offered*
Real Time Acknowledgements	*If Real Time Offered*	*If Real Time Offered*	*If Real Time Offered*	*If Real Time Offered*
Safe Harbor Connectivity and Security	**X**	**X**	**X**	**X**
System Availability	**X**	**X**	**X**	**X**
Companion Guide Template	**X**	**X**	**X**	**X**
Other	N/A	Include guidance for COB in companion guide	Timeframe requirements to process data after successful receipt and verification of transaction	Timeframe requirements to process data after successful receipt and verification of transaction

X = Required

Reminder: Health Claims Attachments transaction not included; there is no formal HIPAA Health Claims Attachments standard(s).

CAQH CORE Connectivity Rule Phases & Applicability to *ASC X12 Transactions*

Evolution --- Each Phase Builds on Previous Phases



Phase IV CAQH CORE 470 Connectivity Rule v4.0.0

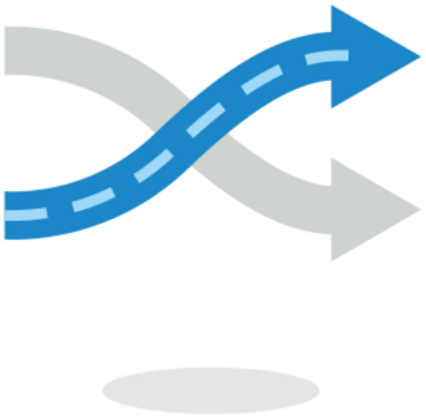
Compatible Safe Harbor

What is Phase IV Safe Harbor?

- A Phase IV Connectivity Rule compliant interface (e.g., that uses X.509 certificate based authentication) must be offered and used if requested by a trading partner.

- However, there is *no requirement* to use a CAQH CORE-compliant method if trading partners agree to use different security requirements, such as a virtual private network (VPN) or secure file transfer protocol (SFTP).

Safe Harbor Principle provides **flexibility** to the industry.

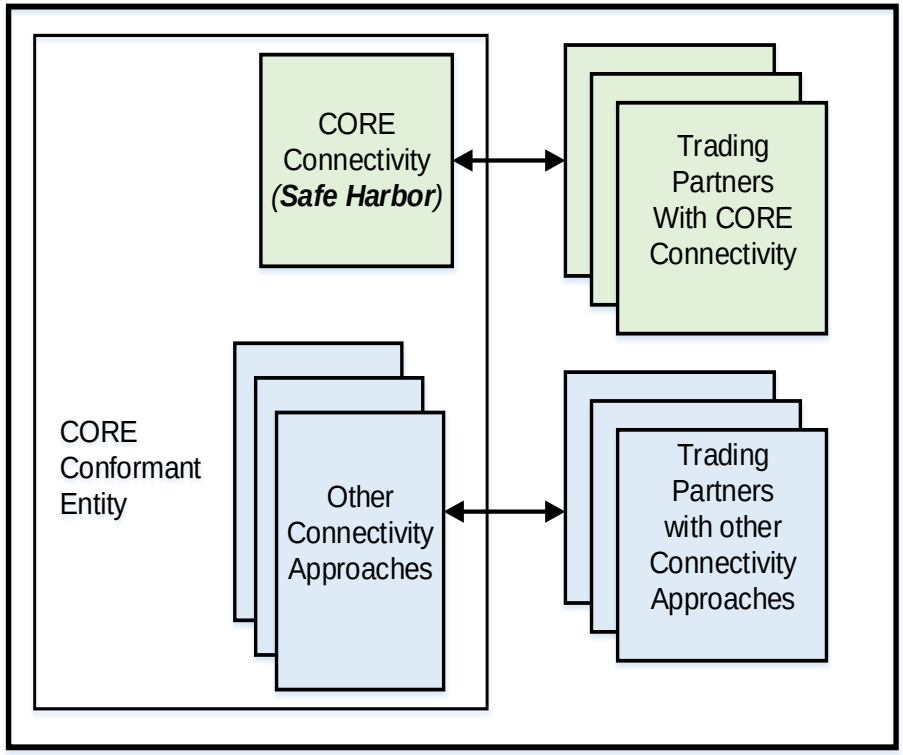


Phase IV CAQH CORE 470 Connectivity Rule v4.0.0

CORE Safe Harbor Principle

The Phase IV CAQH CORE 470 Connectivity Rule v4.0.0 is the connectivity method that a HIPAA covered entity or its agent must implement, and **MUST use if requested by a trading partner for the Phase IV transactions.**

- Enables trading partners to use different communications and security methods than what is specified in rule
- HIPAA covered entities must support CAQH CORE Operating Rule requirements for Real Time and batch processing modes
  - ✓ Can offer other communications and security methods
  - ✓ Does not require trading partners to discontinue any existing connectivity methods not conformant with CAQH CORE Operating Rules



All message payload processing modes specified for the transactions must be supported

- See Phase IV Connectivity Rule §4.4.3.1 and Phase IV CAQH CORE-Required Processing Mode and Payload Type Tables v4.0.0

Polling Question #2

Which of the following would you consider to be the biggest challenge to your organization's implementation of the Phase IV CAQH CORE 470 Connectivity Rule v4.0.0:

1. Fully understanding the requirements of the Phase IV CAQH CORE 470 Connectivity Rule v4.0.0
2. Having enough time and staff for implementation
3. Decision makers have not given the go ahead
4. No major challenges
5. Not applicable

Phase IV CAQH CORE Connectivity Requirement Applicability

Raja Kailar
BNETAL, CEO

Phase IV CAQH CORE 470 Connectivity Rule v4.0.0

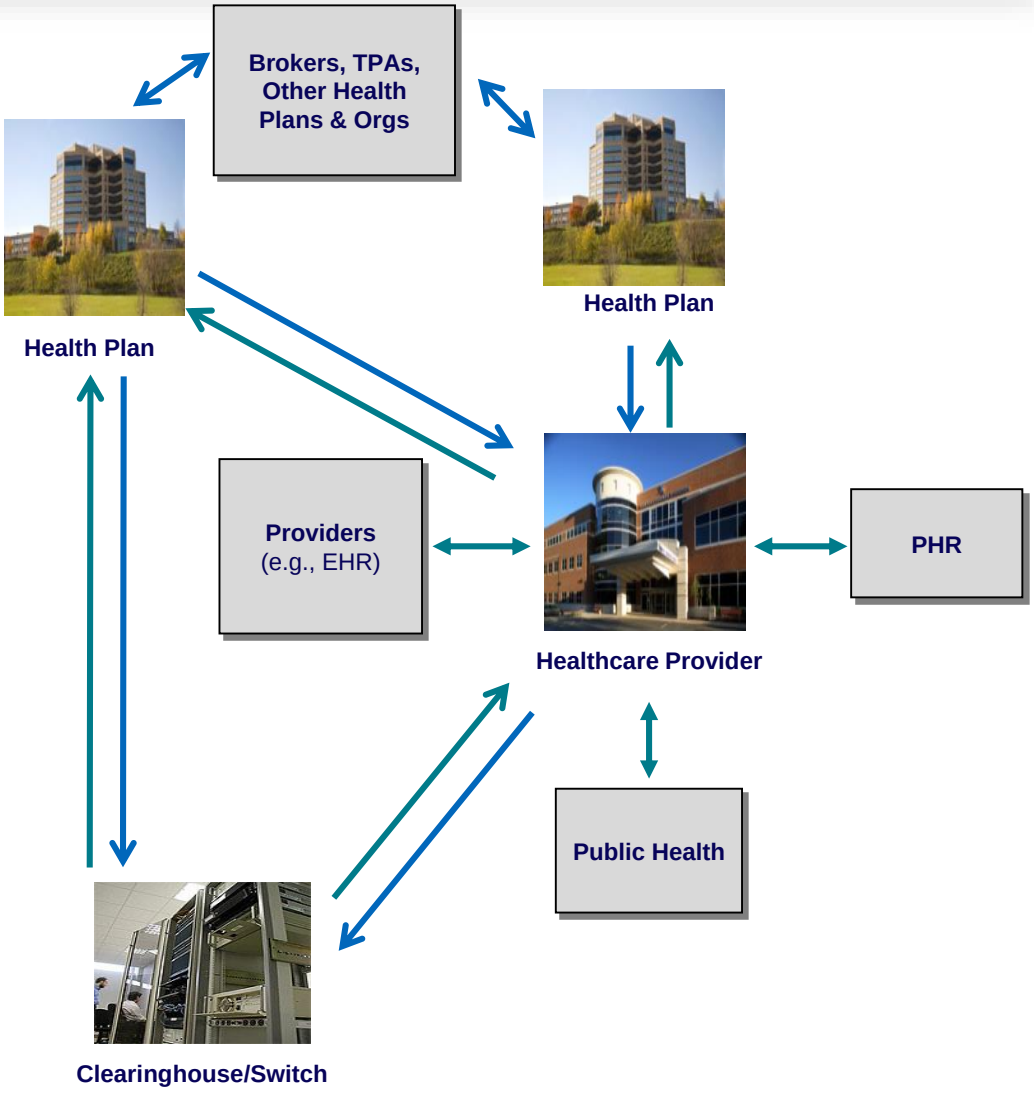
Enhancements to Electronic Transactions

Problem: Multiple connectivity methods are utilized across the industry

- Various connectivity methods for exchanging Claims, Prior Authorization, Benefit Enrollments and Premium Payment transactions - both manual and/or electronic - **drive up transaction costs and increase operational complexity**

Solution: Phase IV CAQH CORE 470 Connectivity Rule v4.0.0

- **Enhances interoperability, efficiency and security by defining technical requirements** for the exchange of the electronic transactions between trading partners so entities can be assured of a common connectivity method



Phase IV CAQH CORE 470 Connectivity Rule v4.0.0

Applicability

Uses the internet as a delivery option and establishes a Safe Harbor connectivity method that is supported by any HIPAA covered entity.

Because of this, the entity is capable and ready at the time of a request by a trading partner to exchange data using the Phase IV CAQH CORE Connectivity Rule.

The Phase IV CAQH CORE Connectivity Rule builds on the Phase II Connectivity Rule to include more prescriptive submitter authentication, envelope specifications, etc.

CORE Safe Harbor applies to:

1. Claims
2. Prior Authorization
3. Benefit Enrollments
4. Premium Payment

Applies to:

Information sources performing role of HTTP/S server

and

Information receivers performing role of HTTP/S client.

Applies to both batch and Real Time transactions. Does not require trading partners to remove existing connections that do not match the rules.

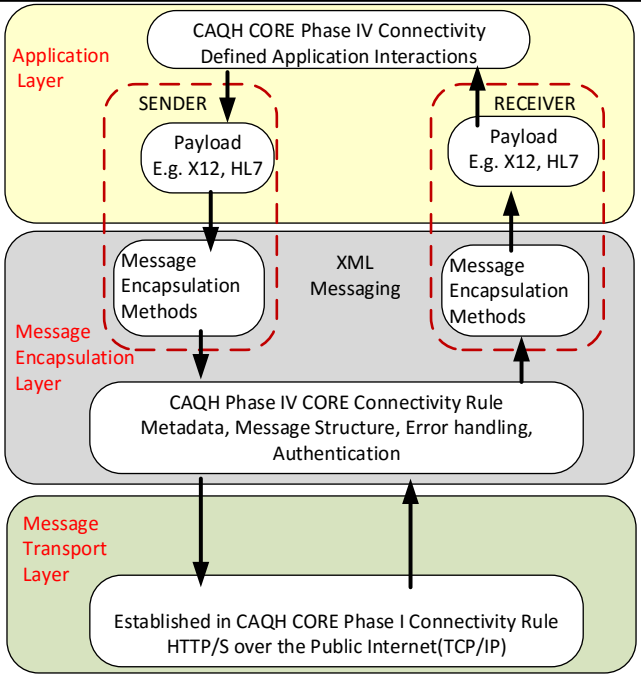
Technical Scope

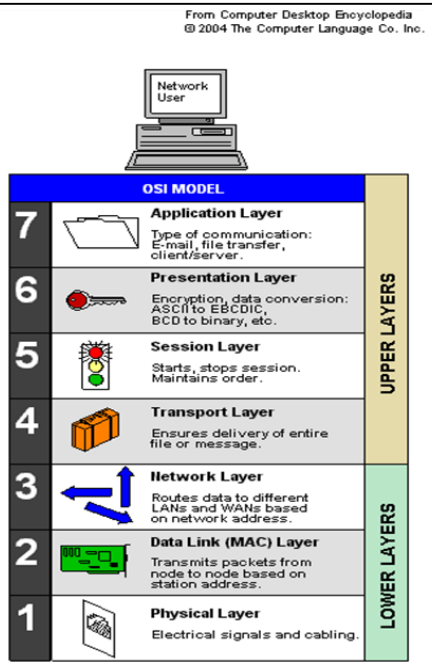
What the Rule Applies To – OSI Model

The scope of the Phase IV CAQH CORE Connectivity rule is specific to:

- OSI Layers 3 and 4 (Transport and Network layers)
- OSI Layers 5 and 6 (Session and Presentation layers, also called Message Encapsulation layers)

Scope is described in terms of the network layers in the Open Systems Interconnection Basic Reference Model (OSI model) (See Rule §3.1)





OSI Model		Messaging Infrastructure Model
Application Layer	OSI 7	Application Layer
Presentation Layer	OSI 6	Message Encapsulation Layer (envelope)
Session Layer	OSI 5	
Transport Layer	OSI 4	Message Transport Layer
Network Layer	OSI 3	

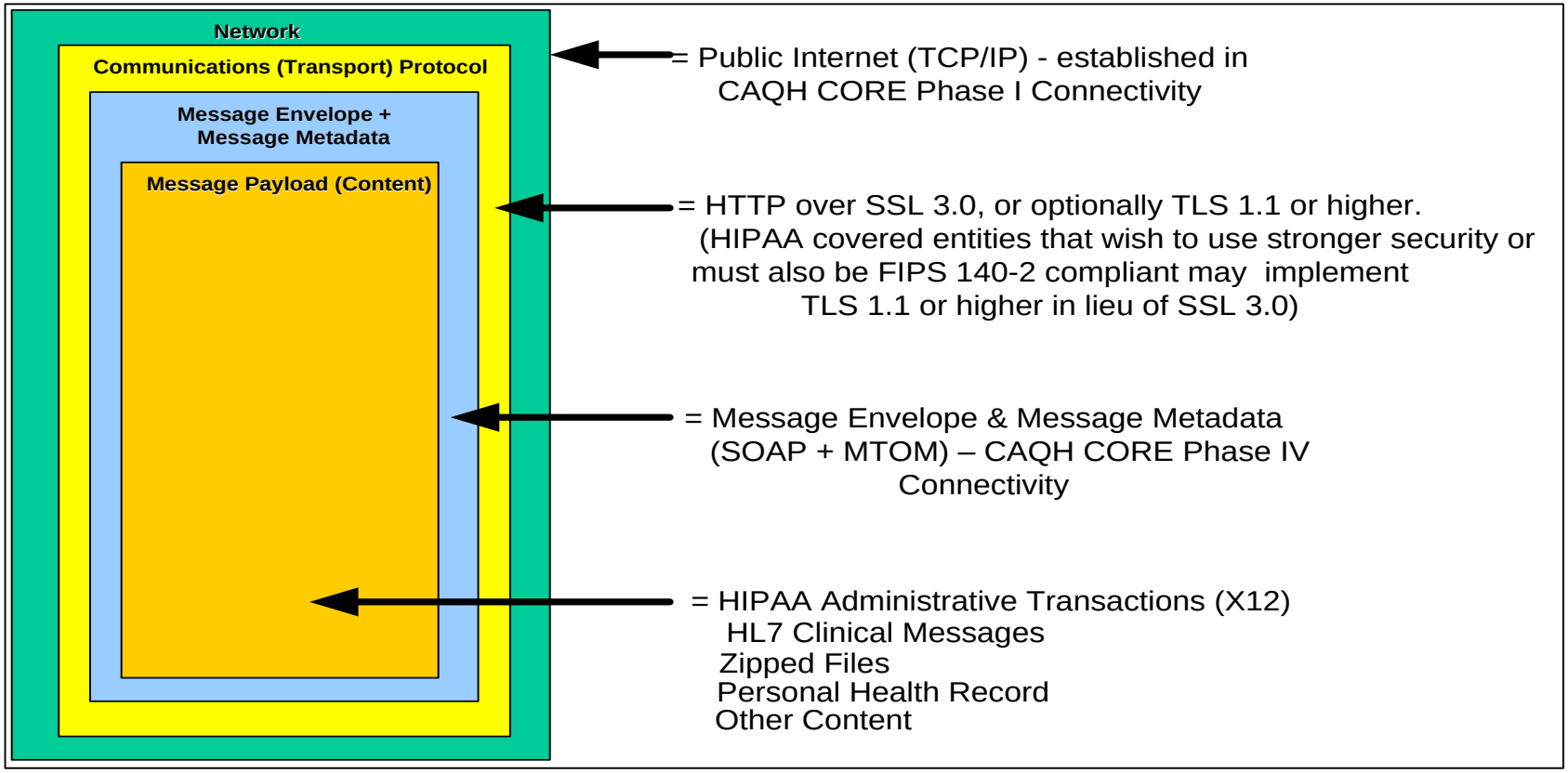
Figure Notes:

- CAQH CORE Phase IV Connectivity Rule addresses Layers 5 and 6 of the OSI Model
- Layer 3 and 4, the Transport Layer and Network Layer, was established as HTTP/S over the public internet in the CAQH CORE Phase I Connectivity Rule
- Layers 1 and 2 are not applicable to CORE because they are not items that could be included in a rule as these layers are so specific to the internal IT systems of every organization.

Technical Scope

What the Rule Applies To – Layered View

The Message Envelope is *outside* the Message Payload (content), and *inside* the Transport Protocol envelope (See Rule §3.1)



- *The Transport Protocol Envelope corresponds to OSI Model Layer 3 and 4*
- *The Message Envelope corresponds to OSI Model Layers 5 and 6*
- *The Message Payload (content) corresponds to OSI Model Layer 7*

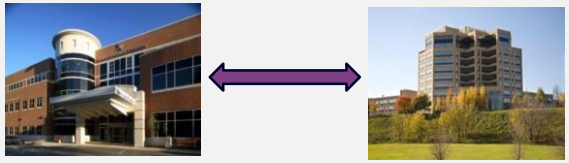
Technical Scope

What the Rule Applies To – Business to Business Connection Models

Interoperability and efficiency is enhanced by the Phase IV CAQH CORE Connectivity Rule's defined technical requirements for exchange of administrative transactions between trading partners, also known as a Business to Business (B2B) relationship

- The Connectivity Rule can be applied independently of the communication architecture or model (e.g., two models are shown below)
- The Connectivity Rule does not apply to Direct Data Entry (DDE) systems

Model 1: B2B Connectivity



Submitter — Health Plan

Model 2: B2B Connectivity with Intermediary

Submitter — Health Plan — Clearinghouse

Not Applicable: Business to Consumer Connectivity

Business

Consumer

CAQH CORE

Stakeholder Conformance Requirements *Specified in Phase IV CAQH CORE Infrastructure Rules*

The Phase IV CAQH CORE Connectivity Rule applies to health plans *(HTTP/S server)* and health care providers *(HTTP/S client)* or their agents, and Clearinghouses *(HTTP/S client)*

- The Phase IV CAQH CORE Infrastructure Rules define conformance requirements for stakeholders based on a typical role (client, server) for message envelope and authentication standards
- The diagram illustrates the typical *(minimal)* roles played by stakeholders (e.g., providers and submitters are typically clients, health plans and TPAs are typically servers, and clearinghouses can act as client or server)

Note: These are the most typical exchanges but other entities may be included in the conduct of the transactions; need to align their role with either client or server as appropriate.

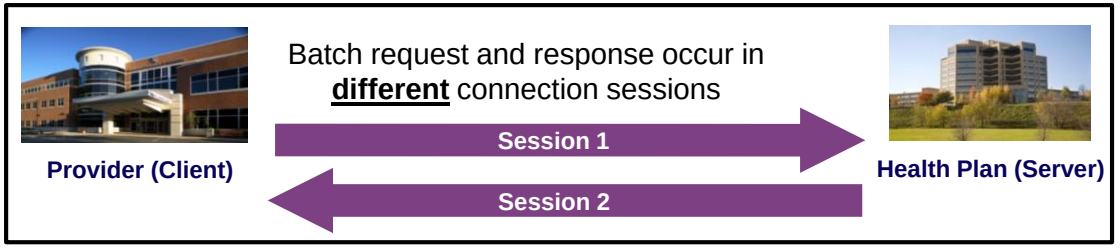
Technical Scope

Synchronous & Asynchronous Message Interactions/Real Time & Batch Processing Modes

The Phase IV CAQH CORE Connectivity Rule addresses synchronous and asynchronous message interaction patterns:

- Message interaction patterns describe how connections are established and used for handling requests and responses

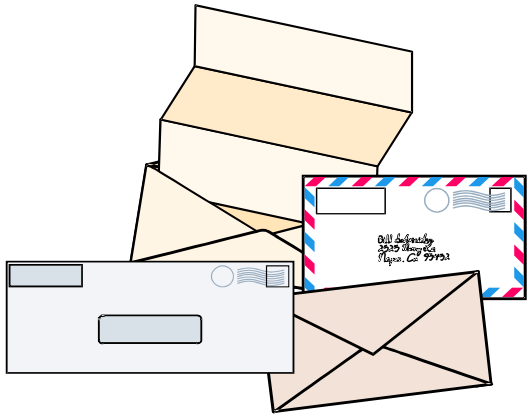
Message Interaction Patterns	Description
Synchronous	• Entity initiates a new connection to send a request; the same connection is used to receive the response for the request • Typically associated with a Real Time mode of processing the message payload
Asynchronous	• Connection is established to send a request; response is sent on a separate connection • Typically associated with a Batch mode of processing the message payload



Message Encapsulation Layer
Envelopes and Metadata

The Message Envelope

- Provides a container for electronic documents (e.g., electronic claims) to be transmitted from the sender to receiver
- Keeps the contents intact, supports auditing/tracking, and provides other critical details
- Needs to include information to identify the sender/receiver (i.e., Message Envelope Metadata) and ensure documents (i.e., Message Payloads) are delivered to the receiver
- Examples of Message Payloads include the HIPAA administrative transactions (ASC X12), HL7 clinical messages and zipped files



Within the CORE Connectivity Rules:

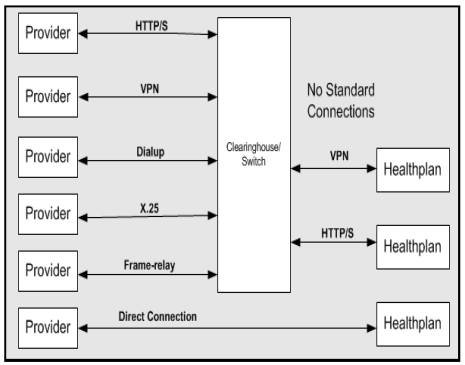
- Message Envelope and Message Envelope Metadata is used primarily to conduct administrative transactions using administrative Message Payloads (e.g., ASC X12 administrative transactions)
- The Message Envelope consists of a well-defined structure for organizing and formatting Message Envelope Metadata
- The Message Envelope Metadata is normative, and helps message receivers route messages for internal processing without opening the envelope, reducing costs and improving response time
- The Message Envelope and Metadata can also be used for non-administrative Message Payloads

CORE Connectivity - *Moving the Industry Forward*

CORE Connectivity common transport and envelope standards reduce implementation variations and improve interoperability and efficiency of administrative transactions

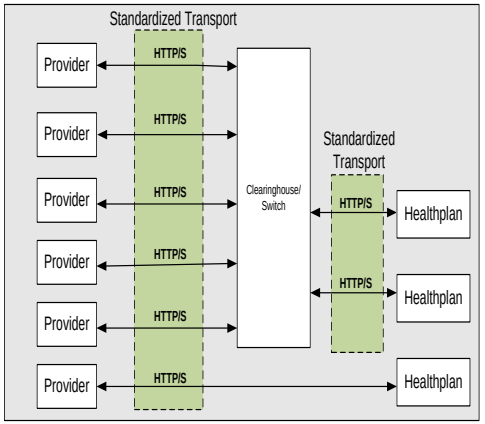
Increased interoperability and improved connectivity

Prior to CORE Connectivity: No Uniform Connection Standard



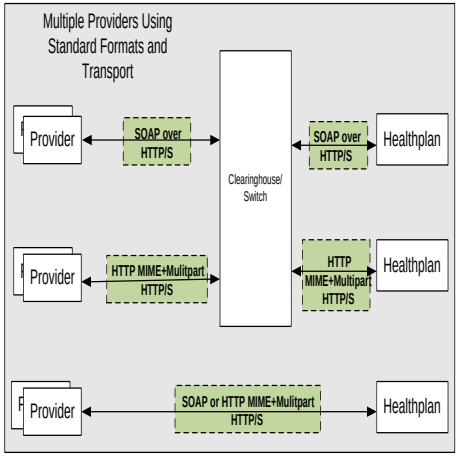
- Costly management of multiple protocols, many proprietary

Phase I CORE Connectivity: Standardized Transport



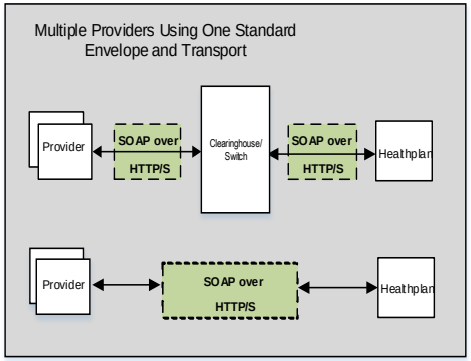
- Greater online access due to uniformity in transport protocols

Phase II CORE Connectivity: Common Transport and Envelope Standards



- Increased and less costly access due to uniformity in transport, envelope, authentication standards, and metadata
- Reduced time spent on implementations and transaction processing time

Phase IV CORE Connectivity: Single Transport & Envelope Standards



- Lower costs due to uniformity in transport, envelope, authentication standards, and metadata
- Reduced time spent on implementations and transaction processing time

CAQH CORE

Phase IV CAQH CORE 470 Connectivity Requirements

Kevin Castellow
BNETAL, Senior Consultant

Phase IV CAQH CORE 470 Connectivity Rule v4.0.0

Key Features

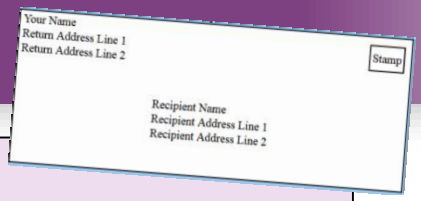
Technical Improvements

- Addresses implementer feedback to improve clarity
- Increases transport security
- Separates payload and processing mode document for easier maintenance
- Simplifies interoperability (convergence to single envelope and authentication standard)
- Contains additional message interactions for conducting new transactions

Transaction Support

- Adds Support for Claims, Premium Payments, Benefit Enrollments and Prior Authorizations
- CORE Safe Harbor allows entities to implement Phase II and/or Phase IV Connectivity for all transactions

Envelope Standard: SOAP+WSDL



SOAP+WSDL

- The Phase IV CAQH CORE 470 Connectivity Rule v4.0.0 supports one envelope standard to attach and send files
- SOAP (Simple Object Access Protocol): a protocol specification for exchanging structured information based on XML using web services
  - XML (Extensible Markup Language): a meta-language that allows users to define their own customized way to describe data; the language used in CAQH CORE Connectivity Rules to create CORE-specific metadata
  - XSD (XML Schema Definition): the schema that defines the data elements in an XML document; the WSDL will rely on the XSD for its definitions
  - Web Services Description Language (WSDL): a document written in XML to describe a Web service (the software system to support machine-to-machine interactions over a network)
- WSDLs describe the web service by detailing the available operations and the data structure needed to use the web service operations

Envelope Standard SOAP+WSDL

Envelope Schema (XSD) Example

```
<?xml version="1.0"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"   xmlns="http://www.caqh.org/SOAP/WSDL/CORERule4.0.0.xsd"
targetNamespace="http://www.caqh.org/SOAP/WSDL/CORERule4.0.0.xsd">
 <xs:element name="COREEnvelopeRealTimeRequest">
  <xs:complexType>
   <xs:sequence>
    <xs:element name="PayloadType" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="ProcessingMode" type="RealTimeMode" minOccurs="1" maxOccurs="1"/>
    <xs:element name="PayloadID" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="TimeStamp" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="SenderID" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="ReceiverID" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="CORERuleVersion" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="Payload" type="xs:base64Binary" minOccurs="1" maxOccurs="1"/>
   </xs:sequence>
  </xs:complexType>
 </xs:element>
 <xs:element name="COREEnvelopeRealTimeResponse">
  <xs:complexType>
   <xs:sequence>
    <xs:element name="PayloadType" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="ProcessingMode" type="RealTimeMode" minOccurs="1" maxOccurs="1"/>
    <xs:element name="PayloadID" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="TimeStamp" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="SenderID" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="ReceiverID" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="CORERuleVersion" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="Payload" type="xs:base64Binary" minOccurs="0" maxOccurs="1"/>
    <xs:element name="ErrorCode" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="ErrorMessage" type="xs:string" minOccurs="1" maxOccurs="1"/>
   </xs:sequence>
  </xs:complexType>
 </xs:element>
```

- XSD snippet to the left shows the Real Time Request and Real Time Response definition with metadata needed for a successful transaction
- Request and Response elements are colored yellow
- Metadata elements are colored in green
  - Metadata elements are defined as optional or required
  - The value type is defined as string or binary

Note: The complete CORE 4.0.0 XSD includes Batch and Generic interaction types which are not shown on this slide

Envelope Standard SOAP+WSDL
WSDL Overview

WSDL Components

Definition: It is the root element of all WSDL documents. It defines the name of the web service, declares multiple namespaces used throughout the remainder of the document, and contains all the service elements described here.

Data types: The data types to be used in the messages are in the form of XML schemas.

Message: It is an abstract definition of the data, in the form of a message presented either as an entire document or as arguments to be mapped to a method invocation.

Operation: It is the abstract definition of the operation for a message, such as naming a method, message queue, or business process, that will accept and process the message.

Port type: It is an abstract set of operations mapped to one or more end-points, defining the collection of operations for a binding; the collection of operations, as it is abstract, can be mapped to multiple transports through various bindings.

Binding: It is the concrete protocol and data formats for the operations and messages defined for a particular port type.

Port: It is a combination of a binding and a network address, providing the target address of the service communication.

Service: It is a collection of related end-points encompassing the service definitions in the file; the services map the binding to the port and include any extensibility definitions.

- The WSDL is an XML coded document that defines the message interactions using the message envelopes defined in the XSD schema.
- Automated tools are able to interpret the XSD and WSDL to generate the necessary source code where logic and additional code is then added.
- The CORE 4.0.0 WSDL is in this link

Envelope Standard SOAP + WSDL

Real Time Request Message Structure (Non-normative-Instructional)

Envelope Standard SOAP + WSDL

Real Time Request Message Structure (Non-normative–Instructional)

CORE Metadata in Use for SOAP 1.2 Request

- The portion of the SOAP envelope in green has the metadata defined in the Phase IV CAQH CORE Connectivity Rule (See §4.4)
- The envelope begins and ends with <soapenv:Envelope> tag
- The envelope contains a <soapenv:Body>
- The metadata from the XSD can be found inside the body element
- Payload element contains the mapping of the xop mapping to the attachment containing the payload content

HTTP Headers

SOAP Envelope

MTOM attachment

```
POST /CORE/PriorAuthRealTime HTTP/1.1
Host: server_host:server_port
Content-Type: multipart/related; boundary= MIMEBoundaryurn_uuid_5117AAE1116EA8B87A1200060184614;
type="application/xop+xml"; start="0.urn:uuid:5117AAE1116EA8B87A1200060184615"; start-
info="application/soap+xml";
action="http://www.caqh.org/SOAP/WSDL/CORETransactions/RealTimeTransaction"

--MIMEBoundaryurn_uuid_5117AAE1116EA8B87A1200060184614
Content-Type: application/xop+xml; charset=UTF-8; type="application/soap+xml"
Content-Transfer-Encoding: binary
Content-ID: <0.urn:uuid:5117AAE1116EA8B87A1200060184615>

<soapenv:Envelope xmlns:soapenv="http://www.w3.org/2003/05/soap-envelope">
        <soapenv:Body>
                <ns1:COREEnvelopeRealTimeRequest
                xmlns:ns1="http://www.caqh.org/SOAP/WSDL/CORERule4.0.0.xsd">
                  <PayloadType>X12_278_Request_005010X217E1_2</PayloadType>
                        <ProcessingMode>RealTime</ProcessingMode>
                        <PayloadID>f81d4fae-7dec-11d0-a765-00a0c91e6bf6</PayloadID>
                        <TimeStamp>2007-08-30T10:20:34Z</TimeStamp>
                        <SenderID>HospitalA</SenderID>
                        <ReceiverID>PayerB</ReceiverID>
                        <CORERuleVersion>4.0.0</CORERuleVersion>
                        <Payload>
                          <xop:Include href="cid:1.urn:uuid:5117AAE1116EA8B87A1200060184692"
                       xmlns:xop="http://www.w3.org/2004/08/xop/include" />
                        </Payload>
                </ns1:COREEnvelopeRealTimeRequest>
                  </soapenv:Body>
</soapenv:Envelope>

--MIMEBoundaryurn_uuid_5117AAE1116EA8B87A1200060184614
Content-Type: image/jpeg
Content-Transfer-Encoding: binary
Content-ID: <1.urn:uuid:5117AAE1116EA8B87A1200060184692>

<Real Time Request Payload (e.g., a payload of type X12_278_Request_005010X217E1_2) goes here>

--MIMEBoundaryurn_uuid_5117AAE1116EA8B87A1200060184614--
```


CAQH CORE

Envelope Standard SOAP + WSDL

Real Time Request Message Structure (Non-normative-Instructional)

Enlarged View

HTTP Headers

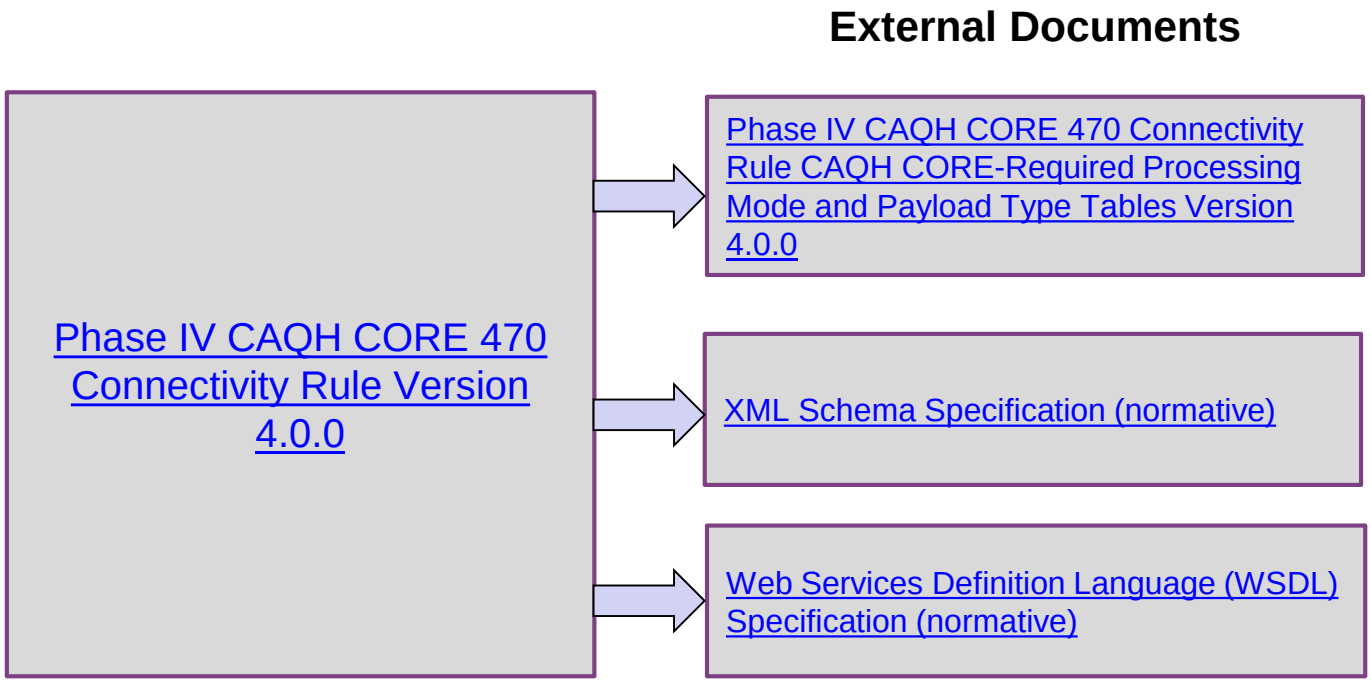
SOAP Envelope

MTOM attachment

```
POST /CORE/PriorAuthRealTime HTTP/1.1
Host: server_host:server_port
Content-Type: multipart/related; boundary= MIMEBoundaryurn uuid 5117AAE1116EA8B87A1200060184614;
type="application/xop+xml"; start="0.urn:uuid:5117AAE1116EA8B87A1200060184615"; start-
info="application/soap+xml";
action="http://www.caqh.org/SOAP/WSDL/CORETransactions/RealTimeTransaction"

--MIMEBoundaryurn uuid 5117AAE1116EA8B87A1200060184614
Content-Type: application/xop+xml; charset=UTF-8; type="application/soap+xml"
Content-Transfer-Encoding: binary
Content-ID: <0.urn:uuid:5117AAE1116EA8B87A1200060184615>

<soapenv:Envelope xmlns:soapenv="http://www.w3.org/2003/05/soap-envelope">
        <soapenv:Body>
              <ns1:COREEnvelopeRealTimeRequest
              xmlns:ns1="http://www.caqh.org/SOAP/WSDL/CORERule4.0.0.xsd">
                <PayloadType>X12_278_Request_005010X217E1_2</PayloadType>
                    <ProcessingMode>RealTime</ProcessingMode>
                    <PayloadID>f81d4fae-7dec-11d0-a765-00a0c91e6bf6</PayloadID>
                    <TimeStamp>2007-08-30T10:20:34Z</TimeStamp>
                    <SenderID>HospitalA</SenderID>
                    <ReceiverID>PayerB</ReceiverID>
                    <CORERuleVersion>4.0.0</CORERuleVersion>
                    <Payload>
                      <xop:Include href="cid:1.urn:uuid:5117AAE1116EA8B87A1200060184692"
                    xmlns:xop="http://www.w3.org/2004/08/xop/include" />
                    </Payload>
              </ns1:COREEnvelopeRealTimeRequest>
                </soapenv:Body>
</soapenv:Envelope>

--MIMEBoundaryurn uuid 5117AAE1116EA8B87A1200060184614
Content-Type: image/jpeg
Content-Transfer-Encoding: binary
Content-ID: <1.urn:uuid:5117AAE1116EA8B87A1200060184692>

<Real Time Request Payload (e.g., a payload of type X12_278_Request_005010X217E1_2) goes here>

--MIMEBoundaryurn_uuid_5117AAE1116EA8B87A1200060184614--
```


CAQH CORE

Phase IV CAQH CORE 470 Connectivity Rule v4.0.0
External Documents



Phase IV CAQH CORE 470 Connectivity Rule v4.0.0

Security

The security aspects of the Rule are intended to assure:

- A message is not altered traveling between trading partner systems
- The message came from a known trading partner

Description of CAQH CORE Connectivity Rules
Connectivity Example with no intermediaries

Messages are protected while traveling to a destination

Submitter (Client)

Client and server must be known to each other in order to send requests

Health Plan (Server)

Note: CAQH CORE Connectivity Rules are a floor, not a ceiling

Phase IV CAQH CORE 470 Connectivity Rule v4.0.0

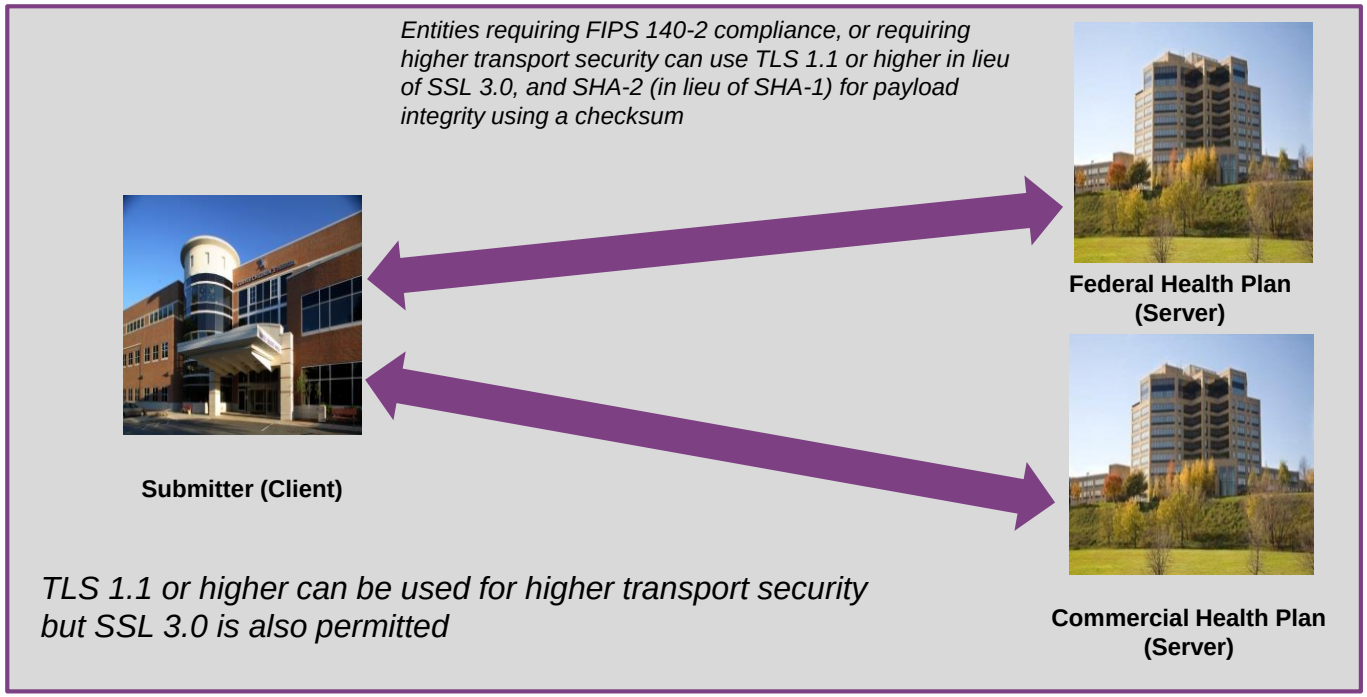
Security Improvements

1. Stronger Submitter Authentication

- X.509 Digital Certificate over SSL/TLS
- Username and Password authentication is removed in this rule

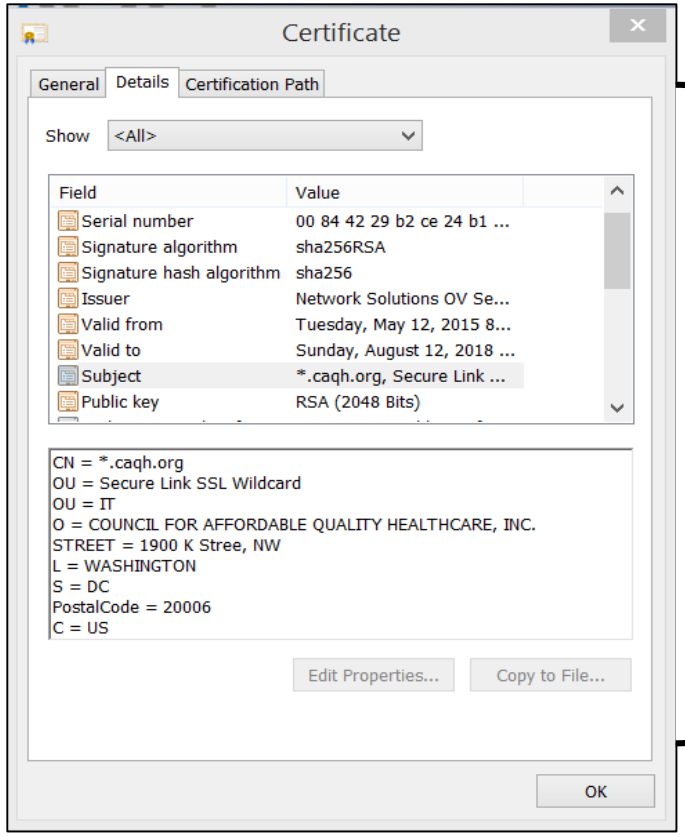
2. Transport Security is enhanced

- Optional use of TLS 1.1 or higher for FIPS 140-2 compliance, or to support an entity's stronger security policy (in lieu of SSL 3.0)
- SHA-2 for payload integrity using a checksum (in lieu of SHA-1)



Transport Layer Security: Digital Certificates

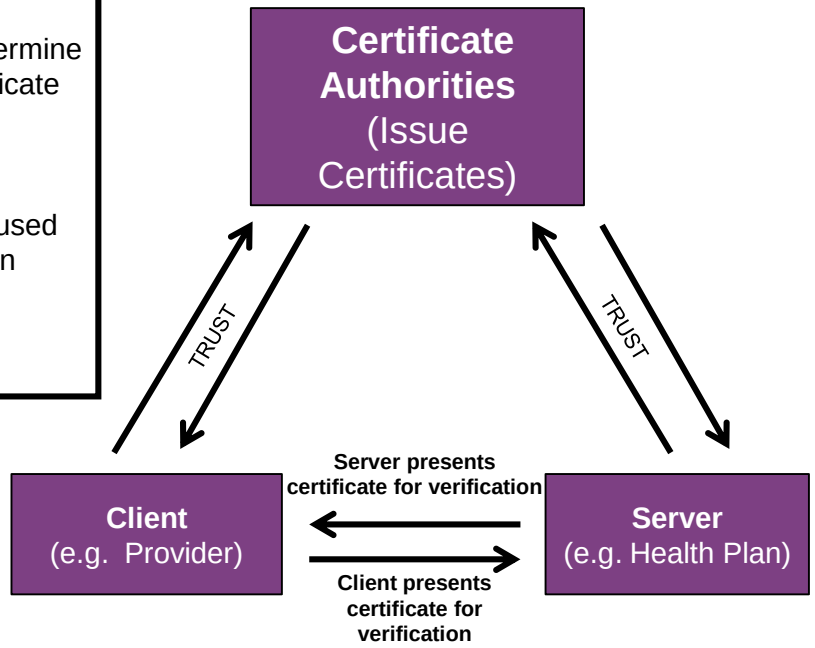
The digital certificate is the proof a server (or a client) provides to a requesting client (or a server) that it is authentic, and not an impersonator.



CERTIFICATE DETAILS

- Subject is the name of the server or could be the name of the client making request. This is the value used in identifying the systems.
- Expiration values that determine the length of use of a certificate in calendar days.
- Cryptographic information stored on the certificate is used to establish random session keys and hashes.

Certificate authorities are trusted based on their security policies and processes.



CAQH CORE

Transport Layer Security: Digital Certificates Lifecycle Considerations

Analysis and Planning Considerations

- Analyze existing Security Policies impacting technical design and implementation decisions
- Identify new Security Policy resources, such as:
  - HealthIT Security Policy Template
  - Federal Security Policy
- Create a Security Policy Document, such as:
  - Digital certificates used for authenticating a system
  - Digital certificates in support of transport security with trading partners
  - Accepted list of certificate vendors

Design and Implementation Considerations

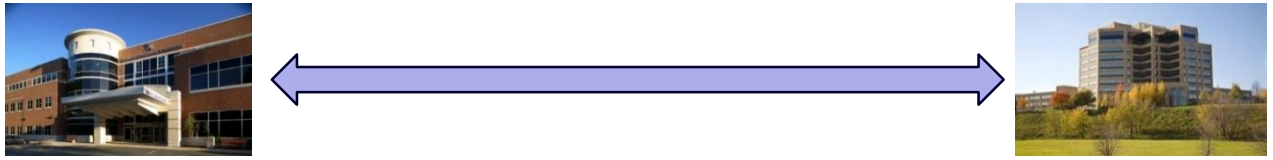
- Develop the certificate infrastructure in-house or outsource (vendors should conform to your certificate policy)
- Create a certificate practice statement (CPS) documenting the use of the digital certificates (NIST CPS document)
- B2B connection authentication can be classified based on identity proofing requirements that an organization uses to issue a Digital Certificate (NIST E-Authentication)

Deployment and Maintenance Considerations

- Negotiate the X.509 digital certificates to use with trading partners
- Manage the X.509 Digital certificate lifecycle, such as:
  - Revoke certificates when the identity of the holder is no longer valid (Digital Certificate Revocation)
  - Renew expired certificates
  - Notify trading partners about certificates to renew or update
  - Assess new regulations, industry trends and best practices, and threat risk assessments; update the certificate infrastructure for these items

Transport Layer: Implementing SSL/TLS

Description of SSL/TLS Connection using a Provider to Health Plan Example



Provider (client) **Health Plan (server)**

- Client certificates are installed at the Provider (client)
- Client certificates contain the Subject value identifying the Provider (client)
- Server certificates are installed at the Health Plan (server)
- Server certificates contain the Subject value identifying the Health Plan (server)

SSL/TLS Basic Steps for Provider/Health Plan Connection Example (Using Mutual Authentication of Client and Server)

1. A Provider (client) initiates a connection to the Health Plan (server).
2. The Health Plan (server) sends its digital certificate to the Provider (client) using connection from step #1.
3. The Provider (client) verifies the Health Plan (server) certificate information.
4. Provider (client) sends client certificate to the Health Plan (server).
5. Health Plan (server) verifies Provider (client) is a known trading partner.
6. A secure connection is established. All information from this point forward is protected within a secure session.

Transport Layer: SSL/TLS Lifecycle Considerations
SSL v3 or (TLS 1.1 or higher)

Analysis and Planning Considerations

- Review national, state, regional and organizational policies; e.g., FIPS 140-2 , NIST Special Publications 800-52r1
- Develop a SSL 3.0 / (TLS 1.1 or higher) policy statement

Design and Implementation Considerations

- Select the set of encryption and signature algorithms that are supported on a server
  - Each version of SSL/TLS supports a different set of algorithms, can constrain the set of algorithms if security policies require
- NIST 800-52 provides implementation considerations for a TLS connection
- Decide if SSL/TLS is implemented in-house or outsourced

Deployment and Maintenance Considerations

- Negotiate using SSL 3.0 or (TLS 1.1 or higher) to use with trading partners

Also See Phase IV CAQH CORE Analysis and Planning Guide

Phase IV CAQH CORE 470 Connectivity Rule v4.0.0
Processing Modes for Transactions

Processing Mode:

- Refers to how the payload of the connectivity message envelope is processed by the receiving system, in Real Time or Batch mode

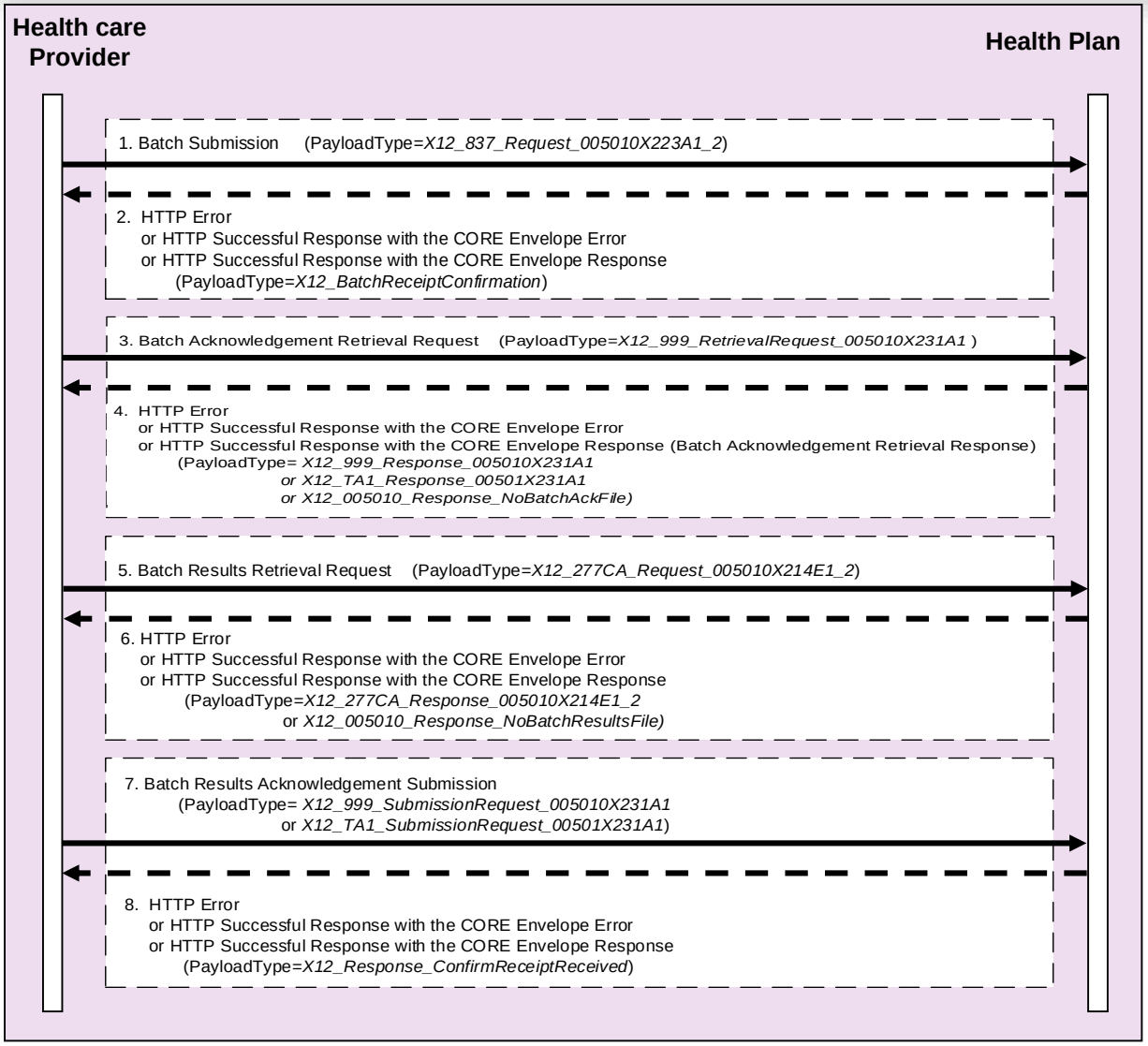
Transaction	Processing Modes
ASC X12N 837 Version 5010 Health Care Claim (Institutional, Professional, Dental)	• Batch Mode Required • Real Time Mode Optional
ASC X12N Version 5010 278 Health Care Services Review – Request for Review and Response	Either Real Time Mode or Batch Mode Must be implemented • Both modes may be implemented
ASC X12N Version 5010 820 Payroll Deducted and Other Group Premium Payment for Insurance Products	• Batch Mode Required • Real Time Mode Optional
ASC X12N Version 5010 834 Benefit Enrollment and Maintenance	• Batch Mode Required • Real Time Mode Optional

Note: The processing modes for the transactions are specified in a separate external document:
Phase IV CAQH CORE 470 Connectivity Rule CAQH CORE-Required Processing Mode and Payload Type Tables v4.0.0 §2 Processing Mode Table

Message Interactions

Batch Processing Claims Example (ASC X12N v5010 837 Claim)

Note: See Phase IV CAQH CORE Rule 470 Connectivity Rule for message interactions for all of the transactions covered by the Phase IV rule set.



Business Transaction Main Flow

1. Provider submits a batch ASC X12N v5010 837 Claim request to the Health Plan.

2. Health Plan responds with a Batch Receipt Confirmation Response.

3. Provider submits a request for the ASC X12C v5010 999 acknowledgement.

4. Health Plan responds with the ASC X12C v5010 999 acknowledgement.

5. Provider submits a request for the ASC X12N v5010 277 Claim Acknowledgement.

6. Health Plan responds with the ASC X12N v5010 277 Claim Acknowledgement.

7. Provider submits a batch results acknowledgment that the ASC X12N v5010 277 Claim Acknowledgement was received.

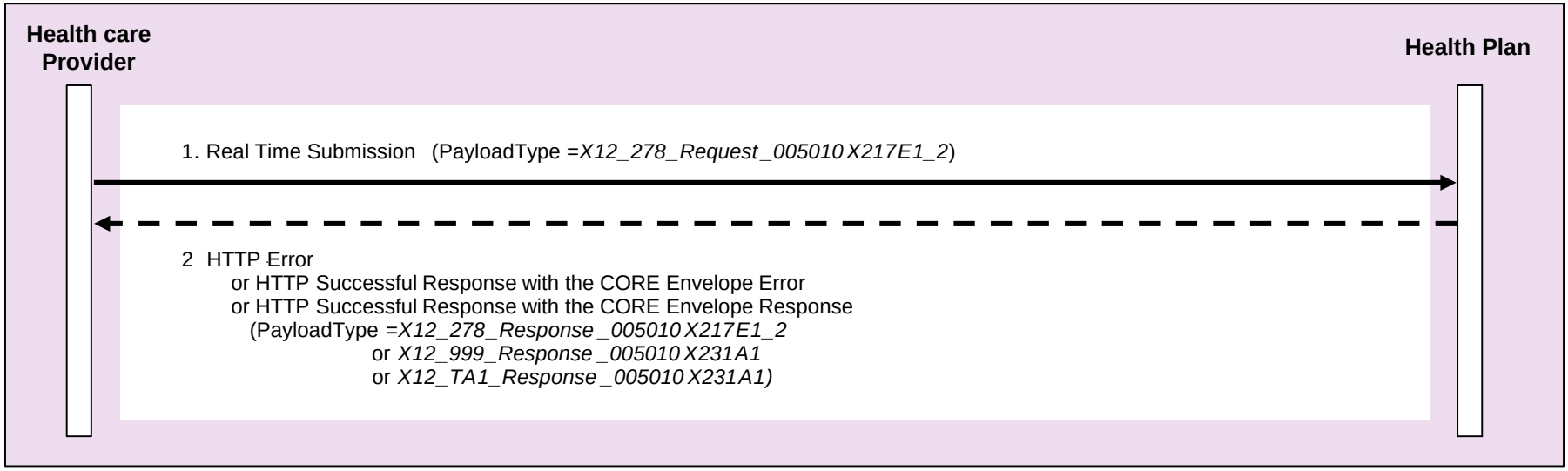
8. Health Plan responds with a receipt confirmation to confirm to the provider the batch results acknowledgement was received.

Message Interactions

Real Time Prior Authorization (ASC X12 v5010 278)

Real Time Processing Mode Example

The payload for a Real Time message interaction consists of a single ASC X12 transaction



Business Transaction Main Flow

1. A Provider submits an ASC X12N v5010 278 Request to a Health Plan

2. A Health Plan responds with an ASC X12N v5010 278 Response to the Provider

Phase IV CAQH CORE 470 Connectivity Rule v4.0.0

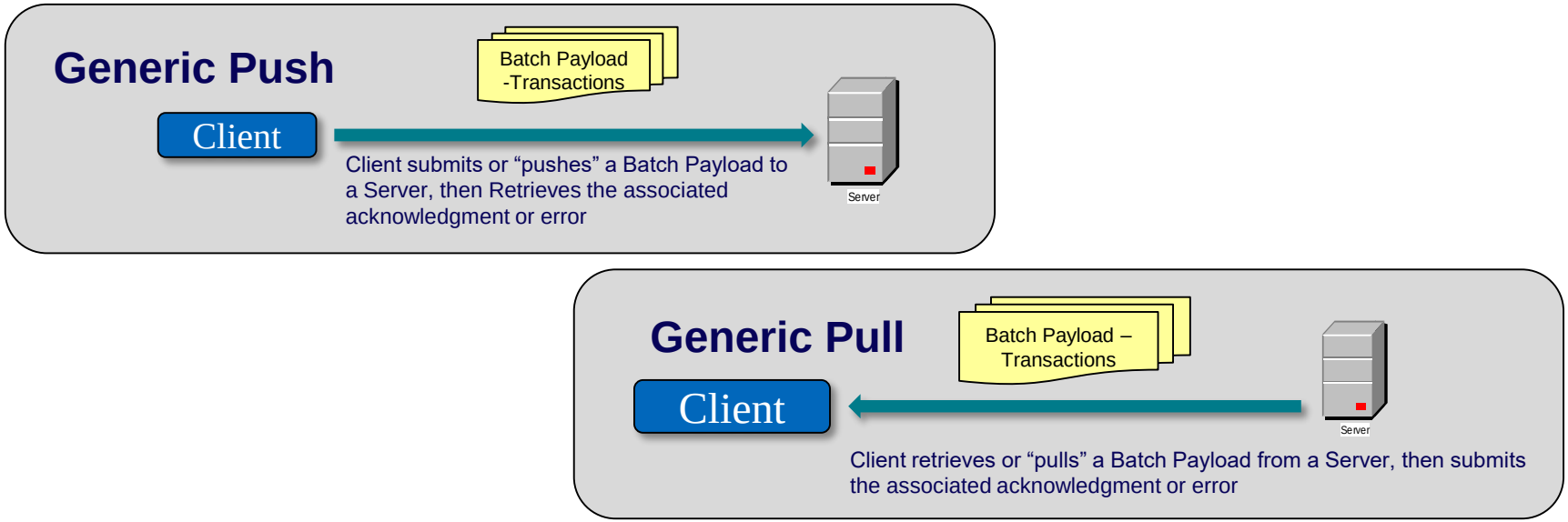
Enhancements to Message Interactions: Generic "Push" & "Pull" Models

The Generic Push and Generic pull message interactions

- The Phase II CAQH CORE Connectivity Rule defined message interactions for conducting Real Time and Batch interactions
- Phase IV CAQH CORE Connectivity Rule keeps the Real Time and Batch interactions and added message interactions that could be used as generic building blocks for supporting current and future transactions
- The Generic Push and Pull Batch Interaction requirements support the conduct of the ASC X12N v5010 834 and the ASC X12N 5010 820 transactions

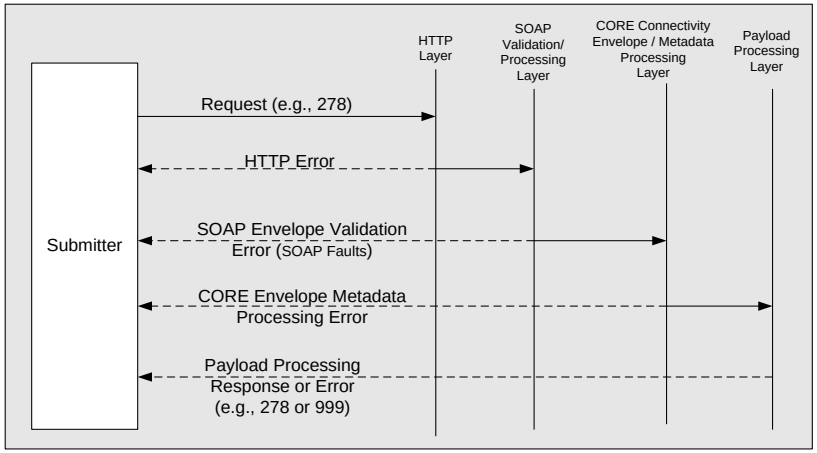
Benefits:

- Provides flexibility to support common industry message interactions for the ASC X12N v5010 820 and ASC X12N v5010 834 where:
  - A Health Plan Sponsor (Client), can "Push" a Batch to a Health Plan (Server)
  - A Health Plan (Client) can "Pull" a Batch from a Health Plan Sponsor (Server)



Phase IV CAQH CORE 470 Connectivity Rule v4.0.0
Error Handling Enhancements

- Error Handling occurs at HTTP, SOAP, CORE Envelope Metadata, and Payload Processing Layers
- CORE Connectivity Rules provides normative error codes and definitions for CORE Envelope Metadata processing
  - ✓ Error handling at HTTP, SOAP and Payload Processing Layers are not defined by CORE
- Phase IV CAQH CORE Connectivity Rule builds on error handling of Phase II CAQH CORE Connectivity Rule:
  - ✓ Addition of error codes based on implementer feedback
  - ✓ Removal of error codes that were required for HTTP+MIME based envelope metadata processing
  - ✓ Added examples and clarified the presentation of the error handling



Error Codes Added	Error description in Rule 470	Reason for Addition
<FieldName>UnSupported	Value is a legal value, but is not supported by the end point receiving the request. Server Connectivity Guide should indicate where to find specific SOAP Operations if multiple URLs are used to support Phase IV CAQH CORE Connectivity.	Implementer feedback from previous phases
NotSupported	A request was received at this server with a valid *PayloadType* or *ProcessingMode* but is currently not implemented by this server (e.g., it may be implemented at a different server within this organization)	Implementer feedback from previous phases

Error Codes Removed	Error description in Rule 270	Reason for Removal in Rule 470
<FieldName>Required	The field <FieldName> is required but was not provided	This is handled by SOAP Fault. Since Rule 470 does not have HTTP+MIME envelope, this error code is longer needed
<FieldName>NotUnderstood	The field <FieldName> is not understood at the receiver.	Same reason as above

Polling Question #3: Additional Education

What CAQH CORE Connectivity topics would you like to learn more about in future CAQH CORE educational webinars?

(Check all that apply)

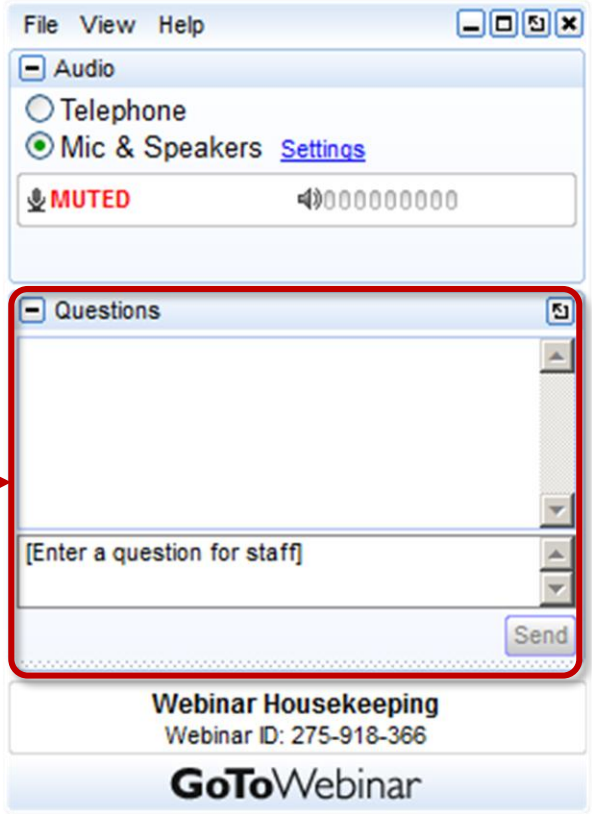
1. Implementer Case Studies
2. Safe Harbor Principle
3. Batch/Real Time Interaction Models

Have other ideas? Let us know! Contact us at CORE@caqh.org

Audience Q & A

Please submit your questions

Enter your question into the “Questions” pane in the lower right hand corner of your screen.



Upcoming CAQH CORE Education Sessions

Going Paperless in your EFT/ERA Transactions – Implementing the Phase III CAQH CORE Operating Rules

THURSDAY, APRIL 28, 2016 – 2 PM ET

CAQH CORE WILL BE JOINED BY THE AMA AND VHA FOR THIS WEBINAR

CAQH CORE Town Hall National Webinar

THURSDAY, MAY 12, 2016 – 2 PM ET

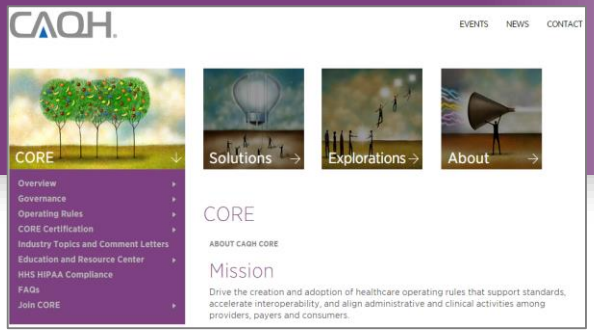
Dialog with PokitDok – How a Healthcare Vendor Has Successfully Implemented the CAQH CORE Operating Rules

FRIDAY, MAY 20, 2016 – 2 PM ET

To register, please go to **www.caqh.org/core/events**

CAQH CORE

Engage with CAQH CORE!



CAQH CORE Website

or contact us at CORE@CAQH.org

Participate in the CAQH CORE Code Combinations Task Group (CCTG) or the Enrollment Data Task Group

Become a CAQH CORE Participating Organization

Explore Voluntary CORE Certification

Register for our educational webinars

Dedicated webpages:

- ✓ Code Combination Maintenance
- ✓ EFT/ERA Enrollment Maintenance
- ✓ Voluntary CORE Certification
- ✓ CAQH CORE Phase IV Operating Rules

CAQH CORE

Thank you for joining us!

Website: www.CAQH.org/CORE

Email: CORE@CAQH.org

@CAQH

Appendix

Appendix Slide List

Slide 48: Server requirements

Slide 49: Security: Improved Support for Security and Compliance

Slide 50: X.509 Digital Certificate: A Single Submitter Authentication Method

Slide 51: ASC X12 Transactions Addressed by Phase IV CAQH CORE Connectivity Rule, Relationship to Previous Phases

Slide 52: Technical Requirements & Relationship to Phase I-III Requirements

Slide 43: Final version of rules

Slide 54: Resource Links

Server Requirements

Server: An entity that receives a message from a Client, which it may process, or relay to another Server

- Ability to receive incoming connections over the public Internet
- Ability to authenticate the incoming connections using the X.509 Client Digital certificate based authentication over SSL Version 3 or TLS 1.1 or higher
- Ability to parse and process the message envelope using the SOAP+WSDL standard as specified in the v4.0.0 XSD and WSDL
- Ability to process the 3rd set of ACA mandated transactions with the processing modes as specified in the Phase IV CAQH CORE-Required Processing Mode and Payload Type Tables v4.0.0
- Ability to receive the payload types specified in the Phase IV CAQH CORE-Required Processing Mode and Payload Type Tables Version 4.0.0 and process the payload types
- Perform error processing
- Track the date, time and payload ID of messages
- Meet the Availability and Response time requirements specified in the CAQH CORE Phase IV Infrastructure Rules
- Publish an Entity-Specific Connectivity Companion Document

Phase IV CAQH CORE 470 Connectivity Rule v4.0.0

Security Across the Layers - Improved Support for Security & Compliance

Transport Security: Security (e.g., authentication, integrity) for electronic transactions conducted over a common medium

- Security requirements:
  - Secure Socket Layer (SSL) Version 3.0 is a standard security technology for establishing an encrypted link between two servers
    - Provides "over the wire" (or transport level) confidentiality and integrity of the data sent over the SSL/TLS session
    - Servers are authenticated using SSL Server Certificates
    - Requires SSL Version 3.0 or optionally TLS 1.1 or higher for transport level security
      - Entities that must also be FIPS 140-2 compliant or whose security policies require enhanced security may implement TLS 1.1 or higher in lieu of SSL Version 3.0.
  - For authenticating clients (i.e., "Submitters"):
    - X.509 Certificates over SSL (optionally TLS 1.1 or higher)
  - For payload integrity verification:
    - SHA-1 A Checksum of the payload is sent as part of the message envelope.
      - Entities requiring FIPS 140-2 compliance may use SHA-2 instead of SHA-1.
      - If SHA-2 is used, then the entity's Connectivity Companion Document can specify that SHA-2 is expected in incoming messages from trading partners.
  - For reliability of transport:
    - UUID* is used for Payload ID (for detecting duplicates)
    - Timestamp is used for ensuring that the data is recent

Related Trends:

- SSL Version 3.0 is commonly used in the industry
- TLS 1.1 or higher is used for securing connections with Federal government trading partners
- HealtheWay - eHealth Exchange (formerly NwHIN Exchange) (included in Meaningful Use-2) uses TLS
- ONC S&I Electronic Submission of Medical Documents (esMD) and Electronic Determination of Coverage (eDoc) use TLS

Phase IV CAQH CORE 470 Connectivity Rule v4.0.0
X.509 Digital Certificate: A Single Submitter Authentication Method

Submitter Authentication

- **X.509 digital certificate** as the single authentication standard
  - Username + password was removed

Benefits:

- X.509 Client Certificate based authentication over SSL/TLS is stronger than username + password
- Reduced implementation cost and complexity having one standard
- Client certificate based authentication requires the submitter to access its cryptographic key (private key) to use its public key certificate
- Digital Certificates
  - expire and need to be renewed, the potential for a successful brute force attack is low
  - can be revoked through a Certificate Revocation List (CRL) or Online Certificate Status Protocol (OCSP) mechanism
- Aligned with clinical initiatives and industry trends (e.g., NwHIN Exchange) that use SOAP over HTTP for clinical data exchanges, and use client certificate based authentication for Business-to Business authentication

Background:

The CAQH CORE Connectivity Rule Version 2.2.0 has two submitter authentication standards:

- X.509 Client Authentication over SSL Version 3.0 or TLS 1.0 (FIPS 140)
- Username-Password

ASC X12 Transactions Addressed by Phase IV CAQH CORE Connectivity Rule, Relationship to Previous Phases

Phase I & II	Phase III	Phase IV
• ASC X12 005010X279A1 Eligibility Benefit Request and Response (270/271) • ASC X12 005010X212 Health Care Claim Status Request and Response (276/277)	• ASC X12 005010X221A1 Health Care Claim Payment/Advice (835) Note: the CAQH CORE Connectivity Rules *do not apply* to the Health Care Electronic Funds Transfers transaction	• ASC X12N 005010X223 Health Care Claim Institutional (837) • ASC X12N 005010X222 Health Care Claim Professional (837) • ASC X12N 005010X224 Health Care Claim Dental (837) *(collectively referred to as ASC X12N 837 v5010 Claim)*
		ASC X12N 005010X217 Health Care Services Review – Request for Review and Response (278) *(generally referred to as Prior Authorization)*
		ASC X12N 005010X218 Payroll Deducted and Other Group Premium Payment for Insurance Products (820) *(generally referred to as Health Plan Premium Payment)*
		ASC X12N 005010X220 Benefit Enrollment and Maintenance (834) *(generally referred to as Benefit Enrollment)*
		***Note:** Although the Phase IV CAQH CORE 470 Connectivity Rule v4.0.0 transactions can be conducted under the Safe Harbor provisions of the either the Phase IV CAQH CORE 470 Connectivity Rule v4.0.0 or the HIPAA-mandated Phase II CAQH CORE 270 Connectivity Rule v2.2.0, all HIPAA-covered entities must still implement the mandated Phase II CAQH CORE Connectivity Rule v2.2.0 for eligibility and claims status.*

Note: References to ASC X12 transactions also include all associated errata

Technical Requirements & Relationship to Phase I-III Requirements

Connectivity Rule Area	CORE Phase I Connectivity Rule Requirements	CORE Phase II & III Connectivity Rule Requirements	CORE Phase IV Connectivity Rule Requirements
Network	Internet	Internet	Internet
Transport	HTTP	HTTP	HTTP
Transport Security	SSL	SSL 3.0 with optional use of TLS 1.x	SSL 3.0, or optionally TLS 1.1 or higher. • Entities that must also be FIPS 140-2 compliant or that require stronger transport security may implement TLS 1.1 or higher in lieu of SSL 3.0
Submitter (Originating System or Client) Authentication	Name/Password	• UserName + Password or • X.509 Digital Certificate	X.509 Digital Certificate based authentication over SSL/TLS • *Removed Username + Password*
Envelope and Attachment Standards	Unspecified	SOAP 1.2 + WSDL 1.1 and MTOM (for Batch) or HTTP+MIME	SOAP 1.2 + WSDL 1.1 and MTOM (for both Real Time and Batch) • *Removed HTTP+MIME*
Envelope Metadata	Unspecified	Metadata defined (Field names, values) (e.g., *PayloadType, Processing Mode, Sender ID, Receiver ID*)	• Metadata defined (Field names, values) (e.g., *PayloadType, Processing Mode, Sender ID, Receiver ID*) • SHA-1 for Checksum • FIPS 140-2 compliant implementations can use SHA-2 for checksum.
Message Interactions/ Routing	• Real-time • Batch (Optional if used)	• Real-time • Batch (Optional if used)	• Batch and Real-Time processing requirements defined for each transaction • Push and Pull Generic messages for 820/834 transactions
Acknowledgements, Errors	Specified	Enhanced Phase I, with additional specificity on error codes	Errors Codes updated
Basic Conformance Requirements for Client and Server Roles	Minimally specified	Well specified	Well specified
Response Time	Specified	Maintained Phase I time requirements	Maintained Phase I time requirements
Connectivity Companion Guide	Specified	Enhanced Phase I, with additional recommendations	Enhanced Phase I, with additional recommendations

Final versions of each rule are available for free on our website (www.CAQH.org/CORE):

Phase IV CAQH CORE 450 Health Care Claim (837) Infrastructure Rule Version 4.0.0

Phase IV CAQH CORE 452 Health Care Services Review – Request for Review and Response (278) Infrastructure Rule Version 4.0.0

Phase IV CAQH CORE 454 Benefit Enrollment & Maintenance (834) Infrastructure Rule Version 4.0.0

Phase IV CAQH CORE 456 Premium Payment (820) Infrastructure Rule Version 4.0.0

Phase IV CAQH CORE 470 Connectivity Rule Version 4.0.0

- XML Schema Specification (normative)
- Web Services Definition Language (WSDL) Specification (normative)
- Phase IV CAQH CORE-Required Processing Mode and Payload Type Tables Version 4.0.0

Resource Links

Sample Resources for Certificate Policies:

- Establish a Certificate Policy (RFC#3647)
- Introduction to Federal PKI NIST Certificate Policy
- Federal PKI Policy - Example CP for digital certificates used by Federal Government entities
- SAFE-BioPharma Certificate Policy - Industry Certificate Policy example
- DirectTrust CP - Example of a healthcare industry specific Certificate Policy

Useful Operational Resources for SSL and TLS

- Guide to Understanding SSL and TLS - Overview of the process to create a secure transport layer
- Securing TLS and SSL Transport - Role of certificates in establishing secure transport and server authentication
- OWASP Transport Layer Security Cheat Sheet
- Testing SSL/TLS Ciphers - Tasks to meet both new regulations and adjust to technology changes