CAQH CORE

Phase IV CAQH CORE Operating Rule Connectivity

Business Value and Technical Implementation with Speakers from PokitDok and BNETAL

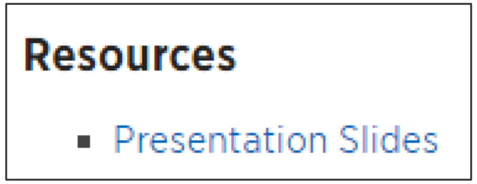
Thursday, November 10th, 2016

2:00 PM ET

Logistics

Presentation Slides & How to Participate in Today's Session

- **Download a copy of today's presentation slides at caqh.org/core/events**
  - Navigate to the Resources section for today's event to find a PDF version of today's presentation slides
  - Also, a copy of the slides and the webinar recording will be emailed to all attendees in the next 1-2 business days

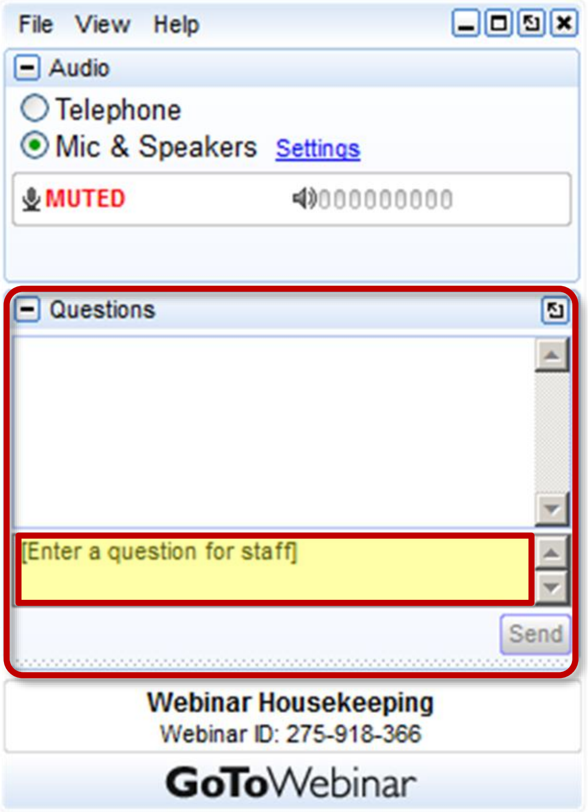


Resources

- Presentation Slides

- 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**



○ Telephone
● Mic & Speakers

MUTED

[Enter a question for staff]

Webinar Housekeeping
Webinar ID: 275-918-366

Thank You Speakers!

CAQH CORE would like to thank our guest presenters for today’s webinar.

Faride Beaubien
Director of EDI Services
PokitDok

Raja Kailar
CEO
BNETAL

Session Outline

- Welcome and Introduction
- Value of Implementing the Voluntary Phase IV CAQH CORE Operating Rules
- PokitDok Phase IV Implementation
- Phase IV CAQH CORE Operating Rules: Connectivity Technical Requirements
- Virtual Dialog with PokitDok and BNETAL
- Audience Q&A

Value of Implementing the Voluntary Phase IV CAQH CORE Operating Rules

Robert Bowman
CAQH CORE Associate Director

Scope of Phase IV CAQH CORE Rule Requirements

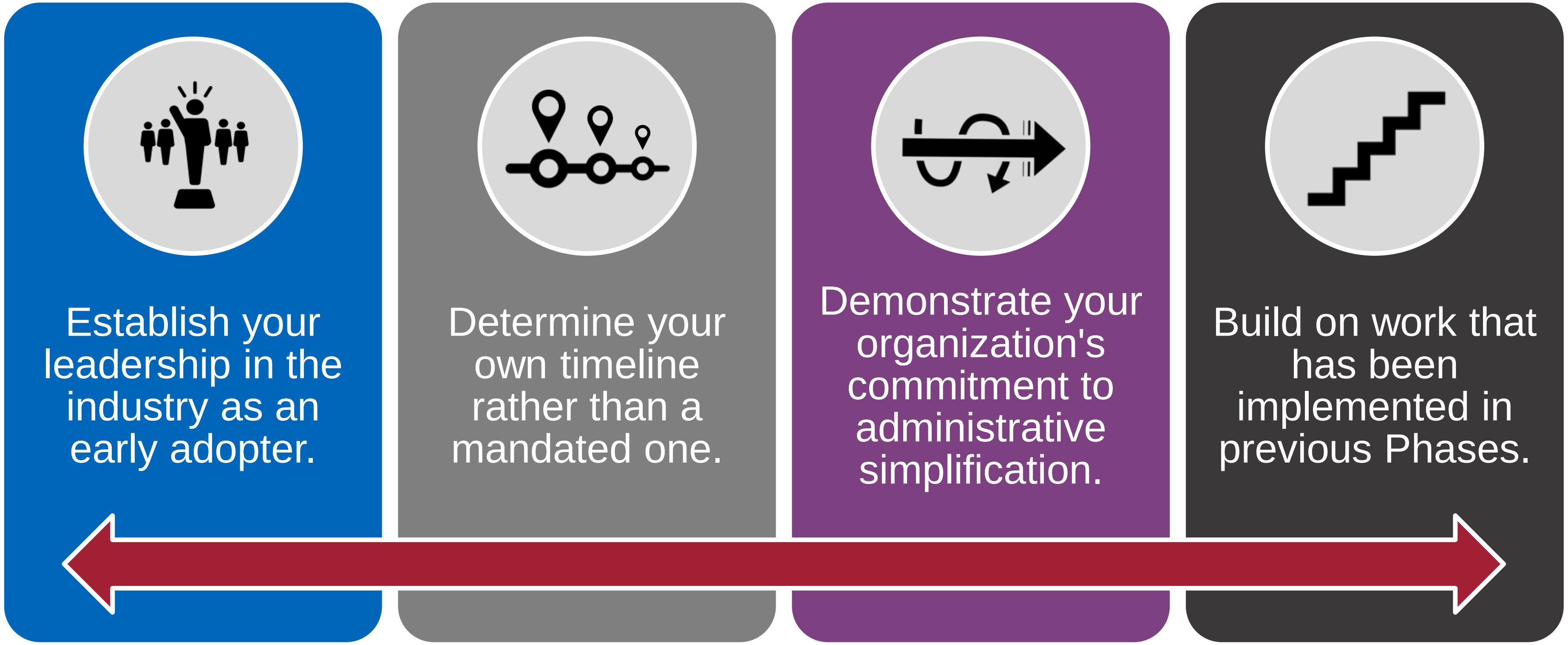
Reminder: Health Claims Attachments transaction not included; there is no formal HIPAA Health Claims Attachments standard(s).

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

Implementing Phase IV CAQH CORE Operating Rules

By voluntarily implementing the Phase IV CAQH CORE Operating Rules, your organization will:



Establish your leadership in the industry as an early adopter.

Determine your own timeline rather than a mandated one.

Demonstrate your organization's commitment to administrative simplification.

Build on work that has been implemented in previous Phases.

Realize savings and efficiencies for you and your customers.

Value Proposition: Cost Reductions/Increased Efficiency

Phase IV Rule requirements will save you time and money

Response time and acknowledgment requirements ensure nothing falls into a black hole and that providers are informed.

Less time is spent verifying information over the phone.

Providers can immediately learn if their claim submissions were successfully received by plan and moved into the adjudication system.

Providers can immediately learn whether the plan has received and is reviewing prior authorization request.

CAQH CORE safe harbor ensures providers can connect online for all of their transactions using their preferred connection method.

Providers can improve coordination of benefits (COB) through more timely eligibility information from health plan and knowledge of plan’s requirement for COB in their companion guide.

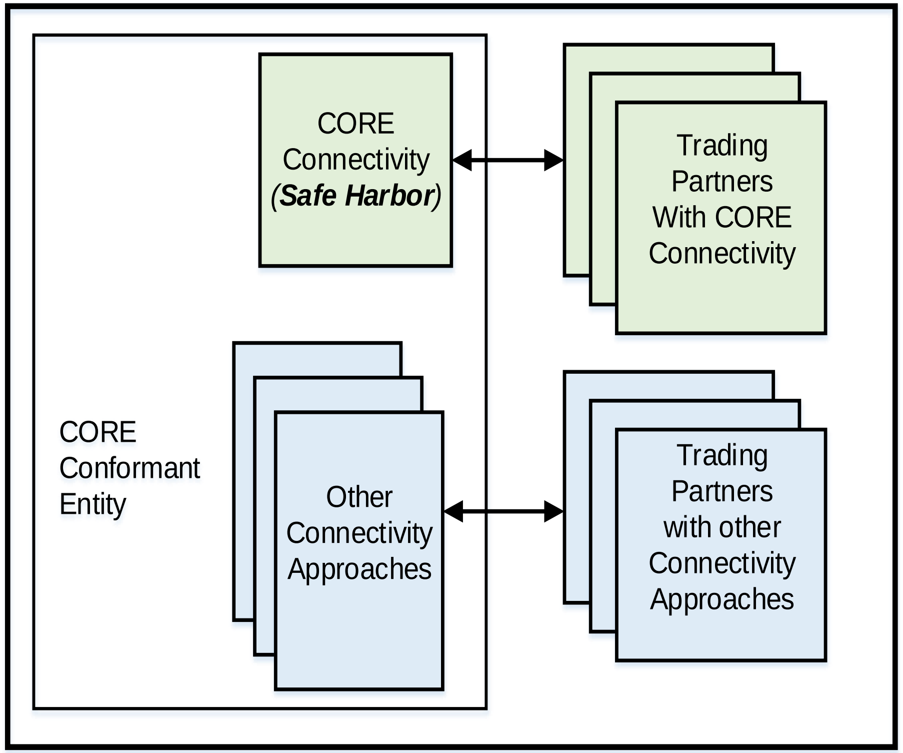
Health plans can build on investments already made in infrastructure for eligibility, claim status, EFT and ERA.

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
- Safe Harbor Principle provides **flexibility** to the industry.
  - ✓ 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).


CORE Connectivity (*Safe Harbor*)
Trading Partners With CORE Connectivity
CORE Conformant Entity
Other Connectivity Approaches
Trading Partners with other Connectivity Approaches

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

pokitdok

Silicon Valley | Silicon Harbor

The Business of Health

What is PokitDok

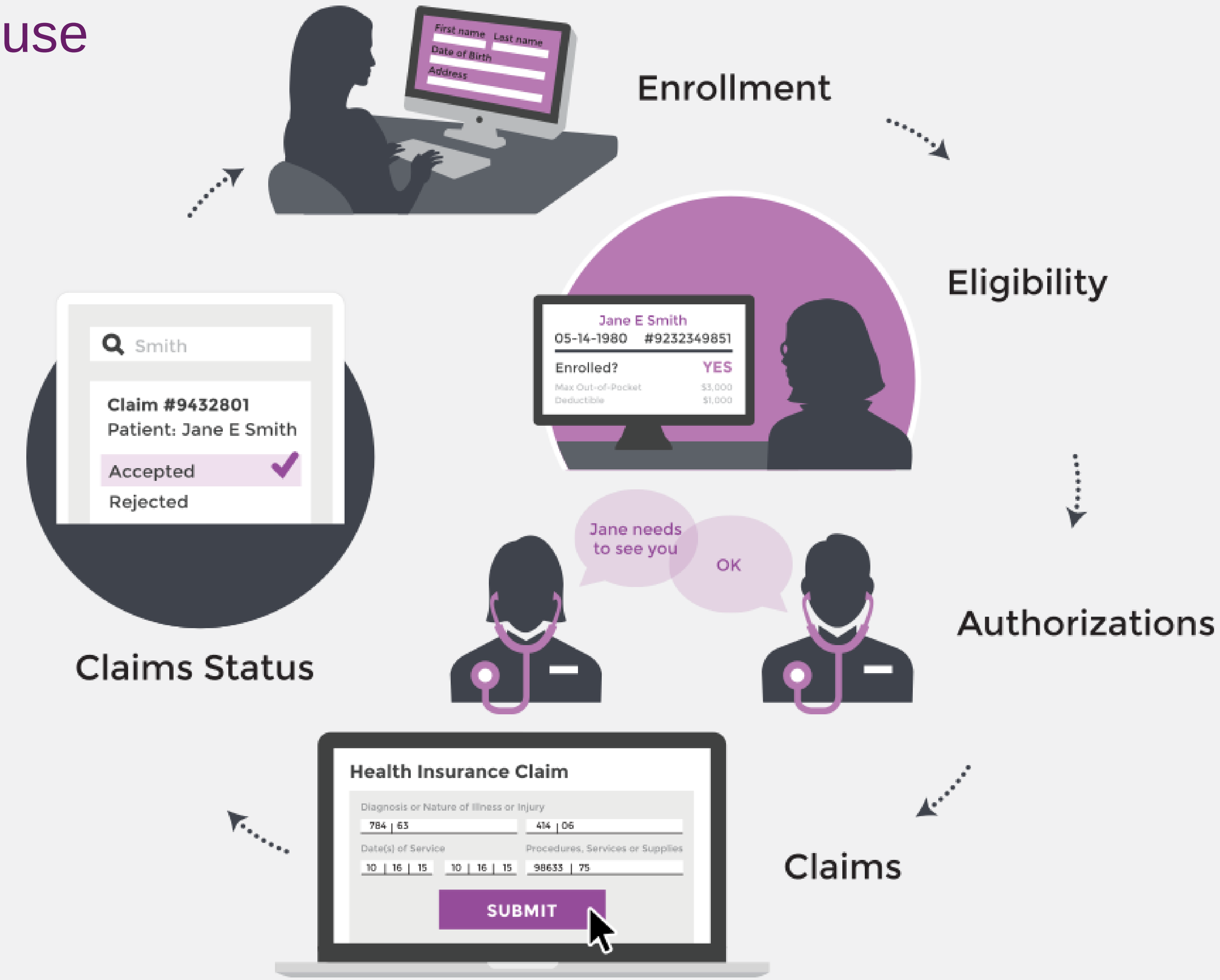
PokitDok connects the business of health
through interoperable cloud-based services
to streamline business operations
and deliver modern patient access solutions.

PokitDok’s mission is to enable the patient experiences, business models and **security** that healthcare deserves through fluid data and modern software.

PokitDok Solutions

- Clearinghouse Services
- Patient Access
- Scheduling
- Identity Management
- Payment Optimization

Clearinghouse Services



First name Last name
Date of Birth
Address

Jane E Smith
05-14-1980 #9232349851
Enrolled? YES
Max Out-of-Pocket $3,000
Deductible $1,000

Health Insurance Claim
Diagnosis or Nature of Illness or Injury
784 | 63 414 | 06
Date(s) of Service
10 | 16 | 15 10 | 16 | 15
Procedures, Services or Supplies
98633 | 75

Smith
Claim #9432801
Patient: Jane E Smith
Accepted ✓
Rejected

PokitDok Security and Compliance

Compliance is native to everything we do.

Technology solutions, business processes, development and delivery protocols are built with integrated security and compliance at their core.

PokitDok meets or exceeds latest security standards.

PokitDok is CAQH Phase I/II/III, HIPAA and PCI compliant.

HiTRUST and EHNAC/CEAP certifications in progress.

PokitDok is a CAQH Phase IV Beta Tester.

CAQH Phase IV

PLANNING

- Reviewed requirements
- Reviewed stakeholder types and differences in requirements
- Assembled a team: EDI Analyst, Software Engineer, DevOps

EXECUTION

- Cross-team collaboration
- Split up tasks

BENEFITS

PokitDok gained an understanding of industry changes
PokitDok was able to proactively plan to make changes

Phase IV CAQH CORE Connectivity Requirement Applicability

Raja Kailar
CEO, BNETAL

Phase IV CAQH CORE 470 Connectivity Rule v4.0.0

Key Features

Technical Improvements

- Added implementer feedback to improve the clarity of the rule wording
- Increases network transport security
- Separates the payload and processing mode documentation into separate documents for easier change maintenance
- Simplifies interoperability
  - Convergence to a single message envelope
  - Single authentication standard
- Contains additional message interactions for conducting additional transactions

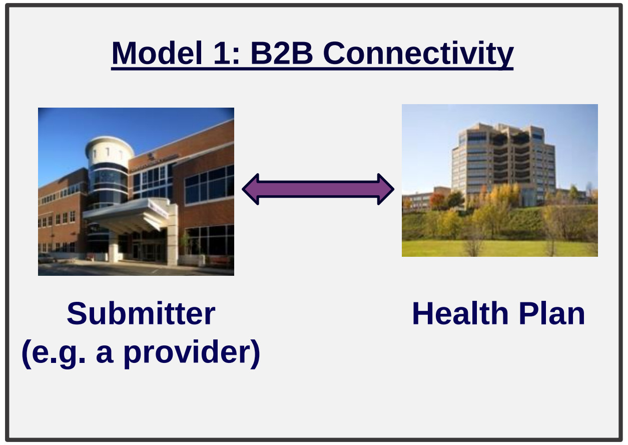
Transaction Support

- Adds support for the Claims, Premium Payments, Benefit Enrollments and Prior Authorizations transactions
- The CORE Safe Harbor allows entities to implement the Phase I, II and/or the Phase IV Connectivity Rules for all transactions, or other connectivity methods

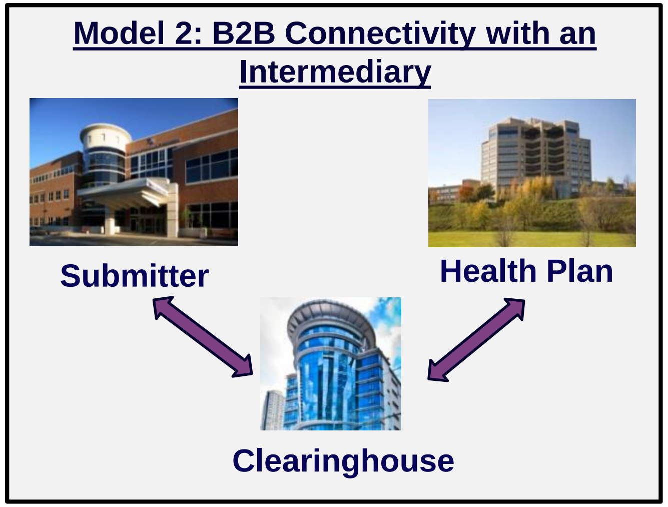
Technical Scope

What the Rule Applies To – Business to Business Connection Models

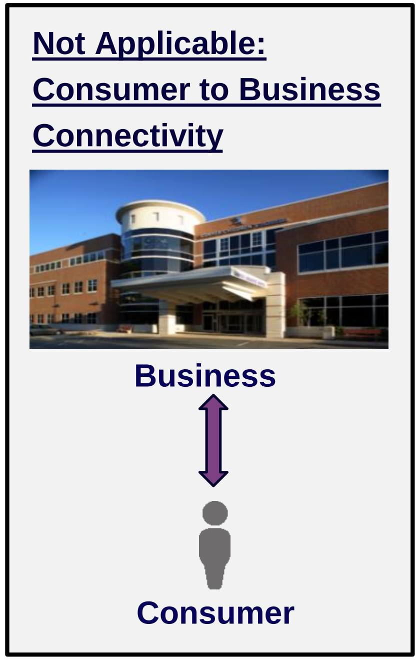
- Trading Partner interoperability and efficiency is enhanced by the Phase IV CAQH CORE Connectivity Rule’s technical requirements for the exchange of administrative transactions, which is known as a Business to Business (B2B) relationship
  - The Connectivity Rule can be applied independently of the trading partners’ communication architecture or model (e.g., two models are shown below)
  - The Connectivity Rule <u>does not</u> apply to Direct Data Entry (DDE) methods (e.g. website input)



Model 1: B2B Connectivity



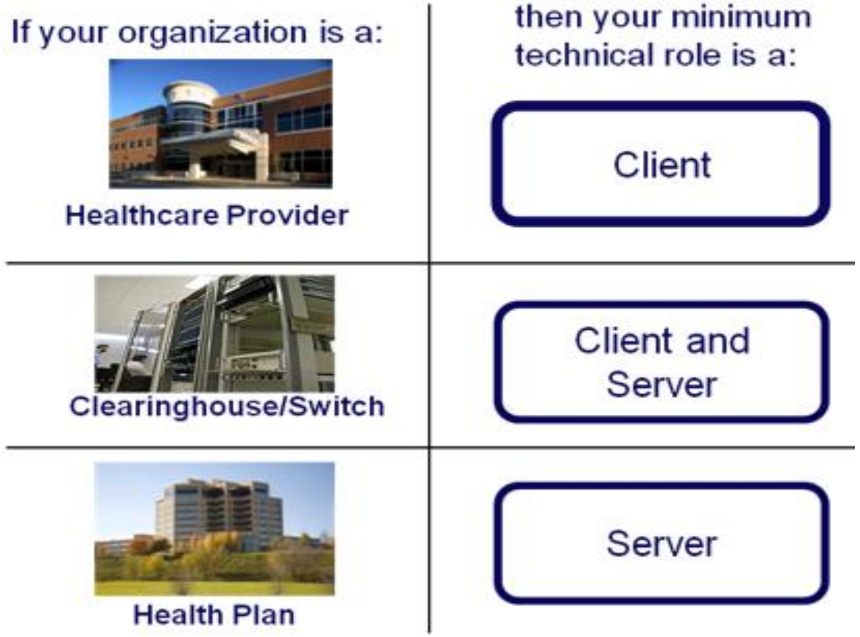
Model 2: B2B Connectivity with an Intermediary



Not Applicable: Consumer to Business Connectivity

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 and/or server)
  - The Phase IV CAQH CORE Infrastructure Rules define the conformance requirements for message envelope and authentication standards, for stakeholder types, based on a typical technical role (client, server)
  - 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 a client or server)



If your organization is a:	then your minimum technical role is a:
Healthcare Provider	Client
Clearinghouse/Switch	Client and Server
Health Plan	Server

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

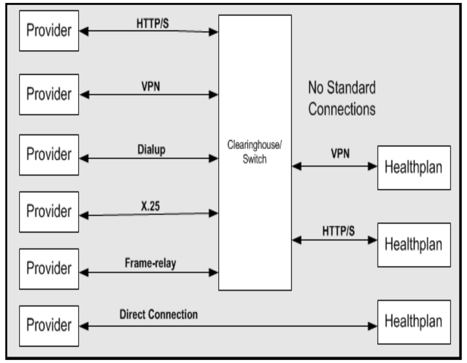
CORE Connectivity

Moving the Industry Forward

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

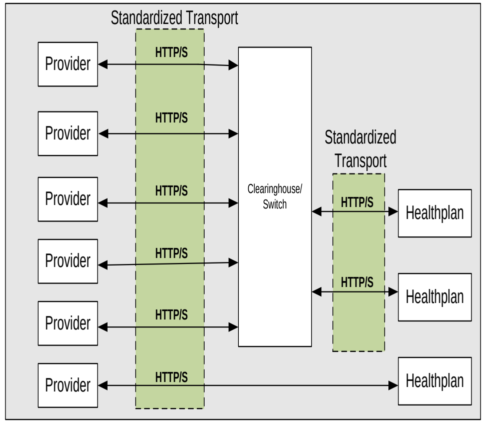
Increased interoperability and improved connectivity

Prior to CORE Connectivity: No Uniform Connection Standard



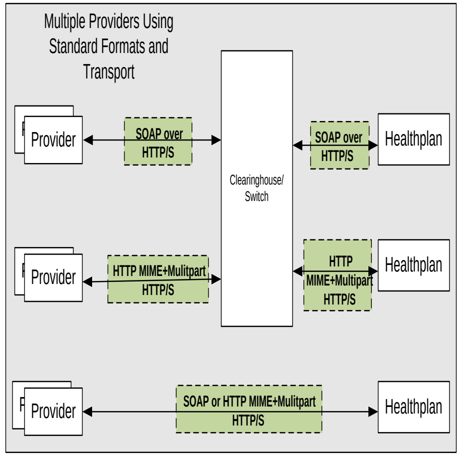
- Costly management of multiple protocols, many proprietary

Phase I CORE Connectivity: Standardized Transport



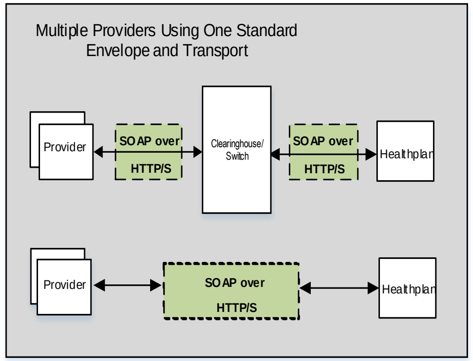
- Greater online access due to an internet transport protocol

Phase II CORE Connectivity: Common Transport and Envelope Standards


Multiple Providers Using Standard Formats and Transport
Provider
SOAP over HTTP/S
Clearinghouse/ Switch
SOAP over HTTP/S
Healthplan
Provider
HTTP MIME+Mulitpart HTTP/S
HTTP MIME+Mulitpart HTTP/S
Healthplan
Provider
SOAP or HTTP MIME+Mulitpart HTTP/S
Healthplan

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

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

Phase IV CAQH CORE 470 Connectivity Requirements

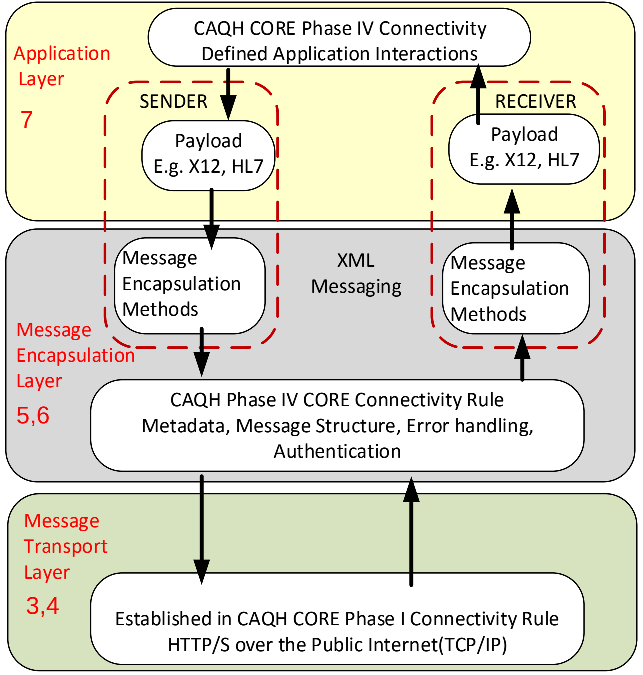
Raja Kailar
CEO, BNETAL

Phase IV CAQH CORE 470 Connectivity Rule v4.0.0 Technical Scope

What the Rule Applies To – OSI Model

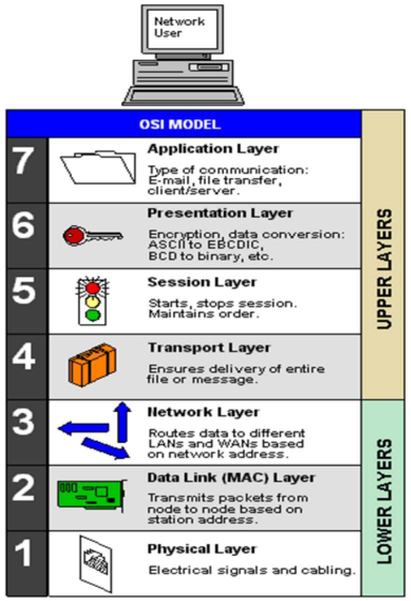
- The scope of the Phase IV CAQH CORE Connectivity rule is specific to:
  - OSI Layers 3 and 4 (Transport and Network layers)
  - OSI Layers 5 and 6 (Session and Presentation layers, also called Message Encapsulation layers)

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



Application Layer
7
CAQH CORE Phase IV Connectivity Defined Application Interactions
SENDER
RECEIVER
Payload E.g. X12, HL7
Payload E.g. X12, HL7
Message Encapsulation Methods
XML Messaging
Message Encapsulation Methods
Message Encapsulation Layer
5,6
CAQH Phase IV CORE Connectivity Rule Metadata, Message Structure, Error handling, Authentication
Message Transport Layer
3,4
Established in CAQH CORE Phase I Connectivity Rule HTTP/S over the Public Internet(TCP/IP)

From Computer Desktop Encyclopedia
© 2004 The Computer Language Co. Inc.



Network User
OSI MODEL
7
Application Layer
Type of communication: E-mail, file transfer, client/server.
6
Presentation Layer
Encryption, data conversion: ASCII to EBCDIC, BCD to binary, etc.
5
Session Layer
Starts, stops session. Maintains order.
4
Transport Layer
Ensures delivery of entire file or message.
3
Network Layer
Routes data to different LANs and WANs based on network address.
2
Data Link (MAC) Layer
Transmits packets from node to node based on station address.
1
Physical Layer
Electrical signals and cabling.
UPPER LAYERS
LOWER LAYERS

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	

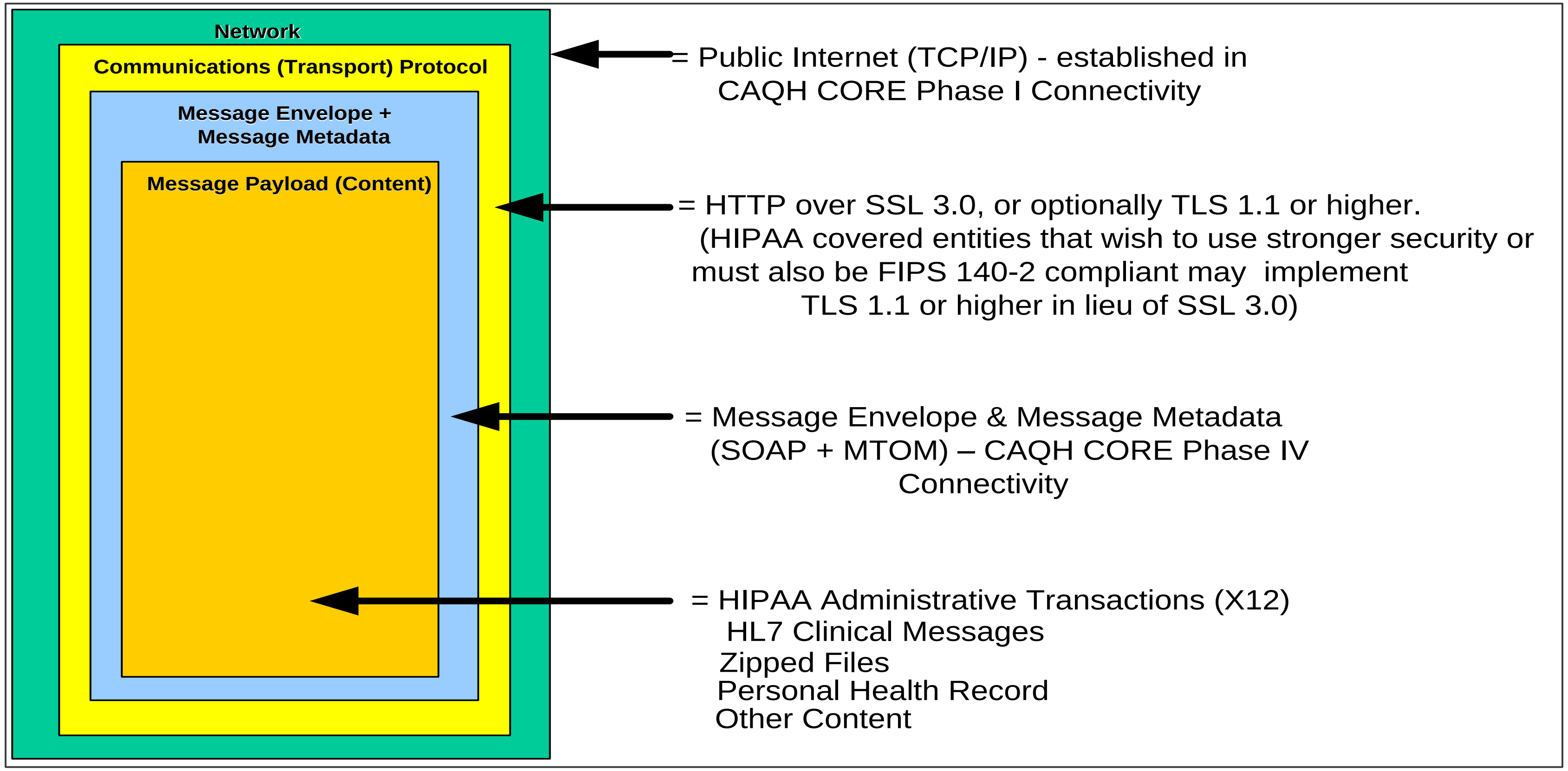
Figure Notes:

- 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.

Phase IV CAQH CORE 470 Connectivity Rule v4.0.0 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)


Network
Communications (Transport) Protocol
Message Envelope +
Message Metadata
Message Payload (Content)

= Public Internet (TCP/IP) - established in CAQH CORE Phase I Connectivity

= HTTP over SSL 3.0, or optionally TLS 1.1 or higher. (HIPAA covered entities that wish to use stronger security or must also be FIPS 140-2 compliant may implement TLS 1.1 or higher in lieu of SSL 3.0)

= Message Envelope & Message Metadata (SOAP + MTOM) – CAQH CORE Phase IV Connectivity

= HIPAA Administrative Transactions (X12)
HL7 Clinical Messages
Zipped Files
Personal Health Record
Other Content

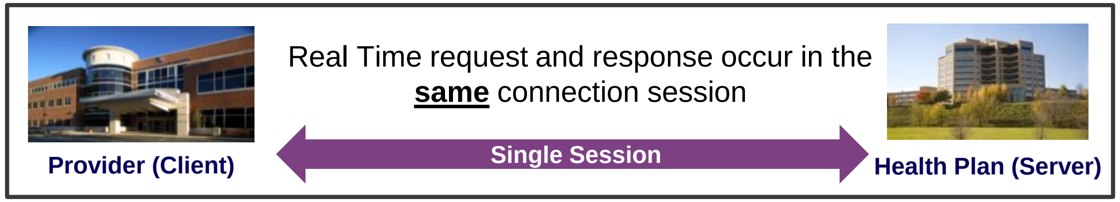
- *The Transport Protocol Envelope corresponds to OSI Model Layer 3 and 4*
- *The Message Envelope corresponds to OSI Model Layers 5 and 6*
- *The Message Payload (content) corresponds to OSI Model Layer 7*

Phase IV CAQH CORE 470 Connectivity Rule v4.0.0 Technical Scope:

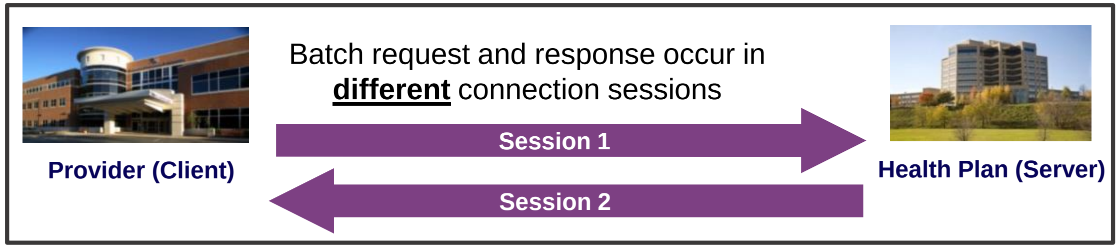
Synchronous & Asynchronous Message Interactions/Real Time & Batch Processing Modes

- 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



Real Time request and response occur in the **same** connection session



Batch request and response occur in **different** connection sessions

Phase IV CAQH CORE 470 Connectivity Rule v4.0.0 Technical Scope:

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

Phase IV CAQH CORE 470 Connectivity Rule v4.0.0

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

Phase IV CAQH CORE 470 Connectivity Rule v4.0.0

Processing Modes for Transactions

Processing Mode:

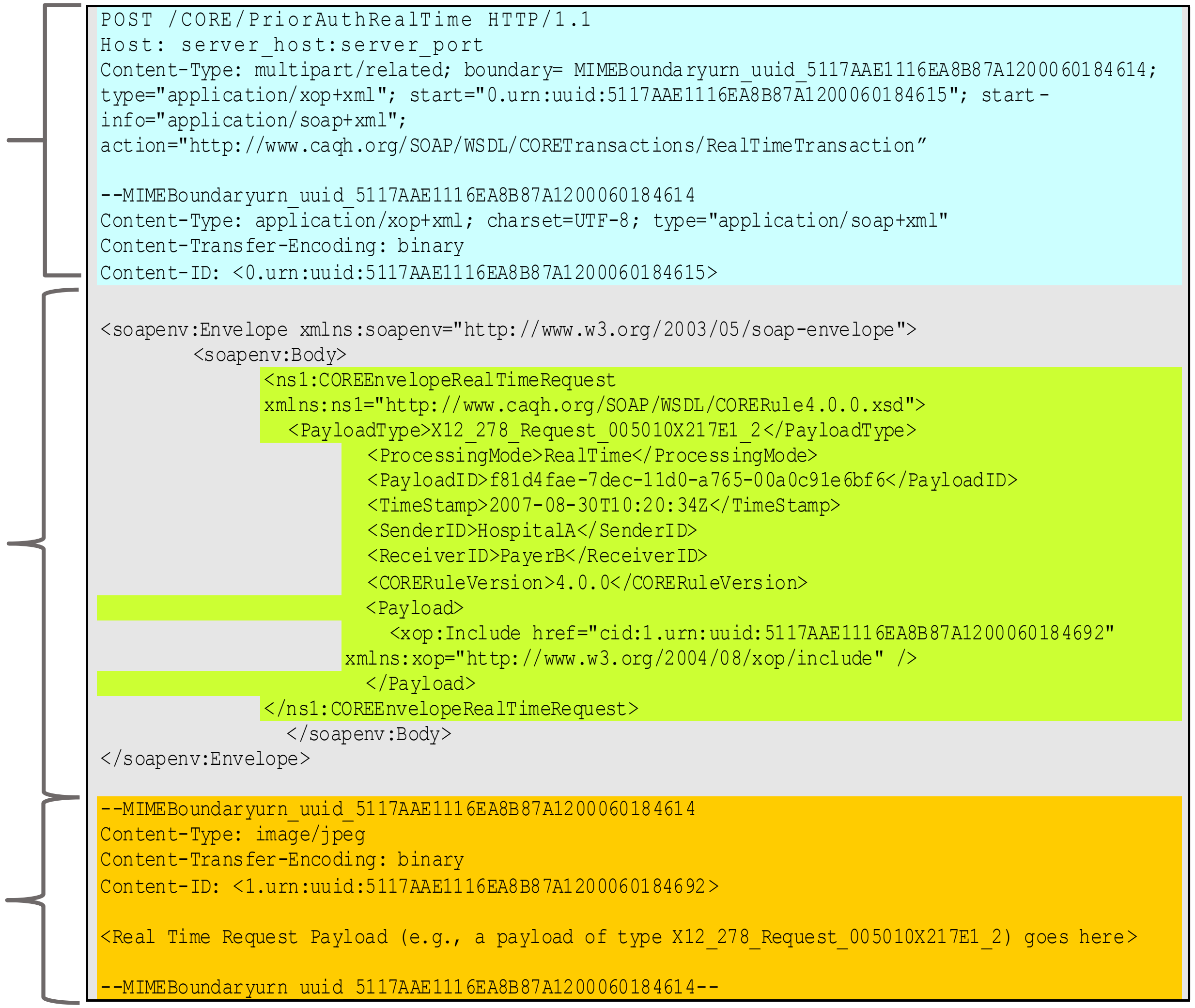
- Refers to how the payload of the connectivity message envelope is processed by the receiving system, in Real Time or Batch mode

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

Phase IV CAQH CORE 470 Connectivity Rule v4.0.0 Envelope Standard SOAP + WSDL

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



HTTP Headers

CORE Metadata in Use for SOAP 1.2 Request

The portion of the SOAP envelope in green has the metadata defined as part of the Phase IV CAQH CORE Connectivity Rule. (See §4.4)

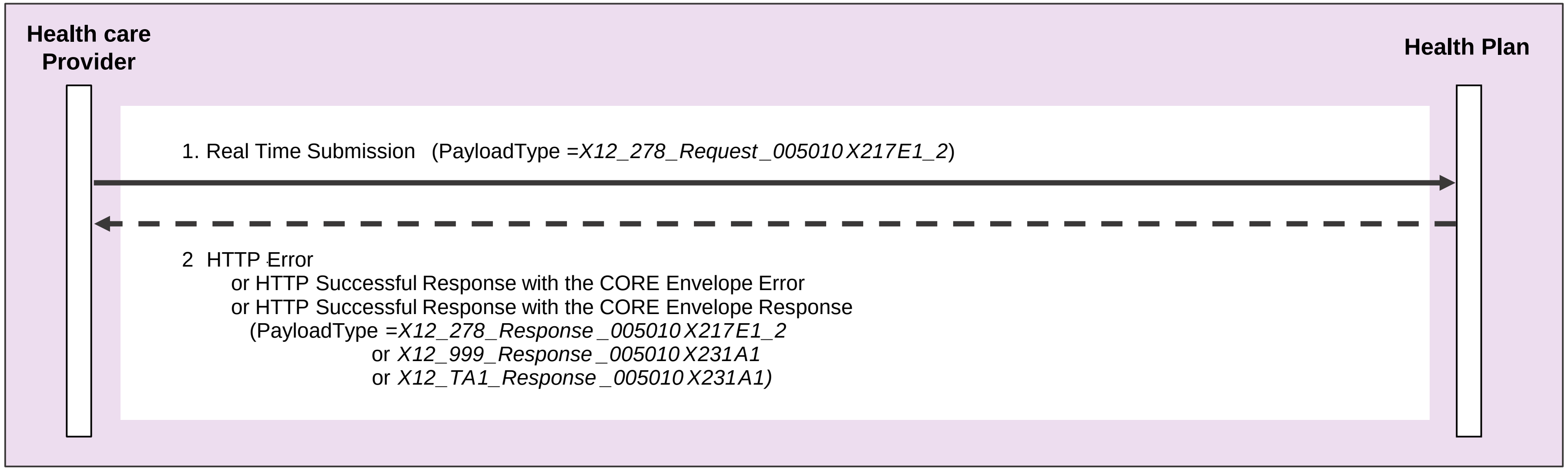
The Real Time Payload file is in orange (MTOM attachment)

```
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--
```

Phase IV CAQH CORE 470 Connectivity Rule v4.0.0 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



Health care Provider

Health Plan

1. Real Time Submission (PayloadType =*X12_278_Request_005010X217E1_2*)

2 HTTP Error
or HTTP Successful Response with the CORE Envelope Error
or HTTP Successful Response with the CORE Envelope Response
(PayloadType =*X12_278_Response_005010X217E1_2*
or *X12_999_Response_005010X231A1*
or *X12_TA1_Response_005010X231A1)*

Business Transaction Main Flow

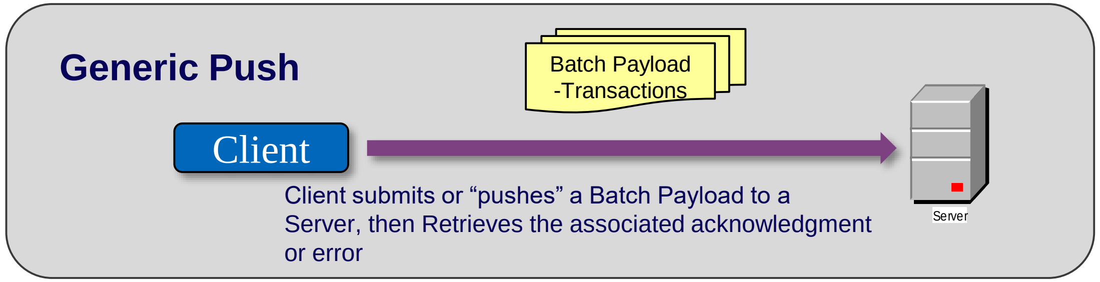
1. A Provider submits an ASC X12N v5010 278 Request to a Health Plan ———

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

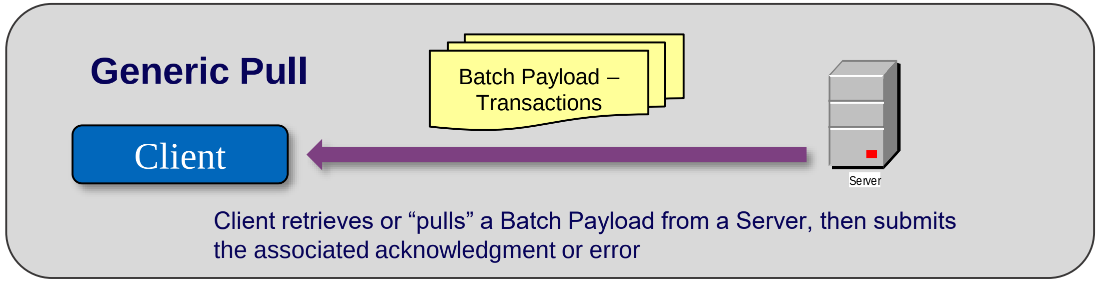
Generic “Push” and “Pull” Batch Processing Mode Message Interactions

- **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)



Generic Push

Client submits or “pushes” a Batch Payload to a Server, then Retrieves the associated acknowledgment or error



Generic Pull

Client retrieves or “pulls” a Batch Payload from a Server, then submits the associated acknowledgment or error

Phase IV CAQH CORE 470 Connectivity Rule v4.0.0

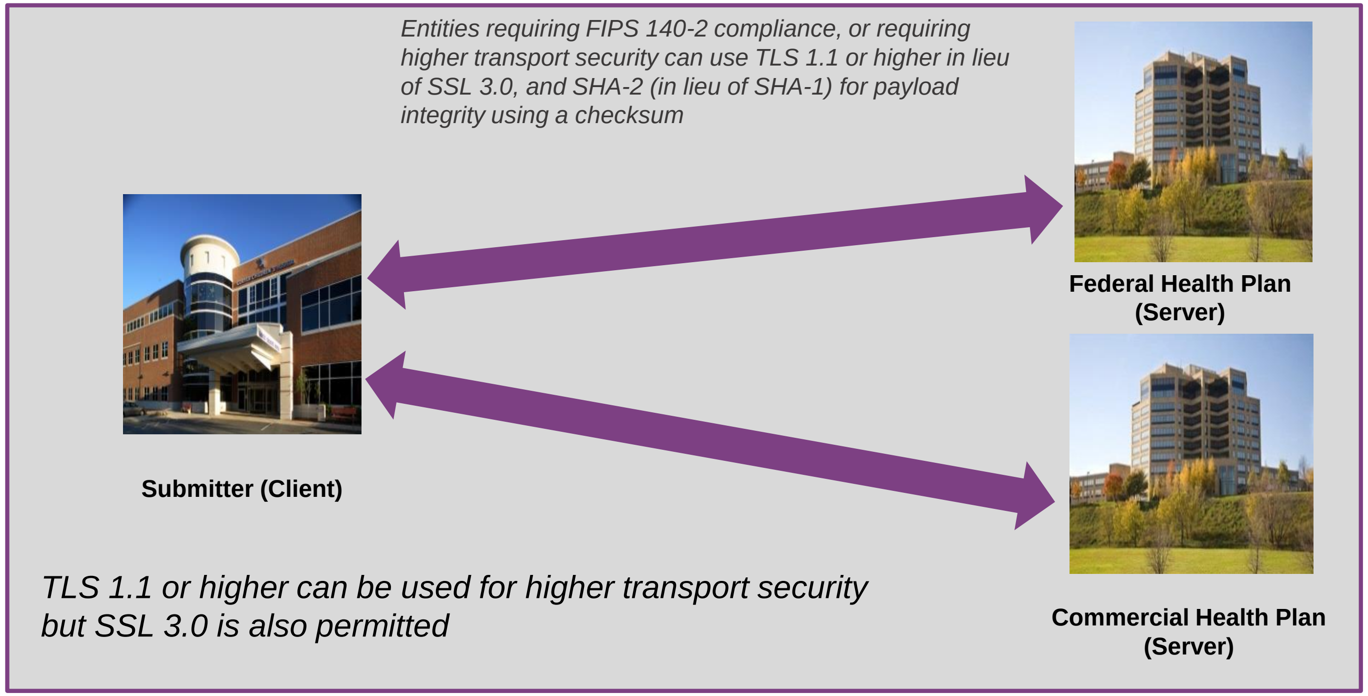
Security Requirements

1. Submitter Authentication

- X.509 Digital Certificate over SSL/TLS
- Username and Password authentication has been phased out in this rule

2. Transport Security

- SSL Version 3 or TLS 1.1 or higher (TLS 1.1 or higher can be used in addition to or in lieu of SSL 3.0 for FIPS 140-2 compliance, or to support an entity’s stronger security policy)
- SHA-2 for payload integrity using a checksum (in lieu of SHA-1)



Entities requiring FIPS 140-2 compliance, or requiring higher transport security can use TLS 1.1 or higher in lieu of SSL 3.0, and SHA-2 (in lieu of SHA-1) for payload integrity using a checksum

TLS 1.1 or higher can be used for higher transport security but SSL 3.0 is also permitted

Polling Question #1

What voluntary Phase IV CAQH CORE Operating Rule implementation planning stage(s) do you plan to complete by the end of 2017? (Select all that apply)

1. Internal Education and Awareness
2. Analysis and Planning/Systems Design
3. Systems Implementation/Integration and Testing
4. Deployment/Maintenance
5. No Plans/Unsure

Virtual Dialog with PokitDok and BNETAL

Moderator
Jessica Porras
CAQH CORE Senior Manager

Virtual Dialogue with PokitDok and BNETAL

Faride Beaubien
Director of EDI Services
PokitDok

Raja Kailar
CEO
BNETAL

Robert Bowman
CAQH CORE Associate Director

Taha Anjarwalla
CAQH CORE Senior Associate

Jessica Porras
CAQH CORE Senior Manager
MODERATOR

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:

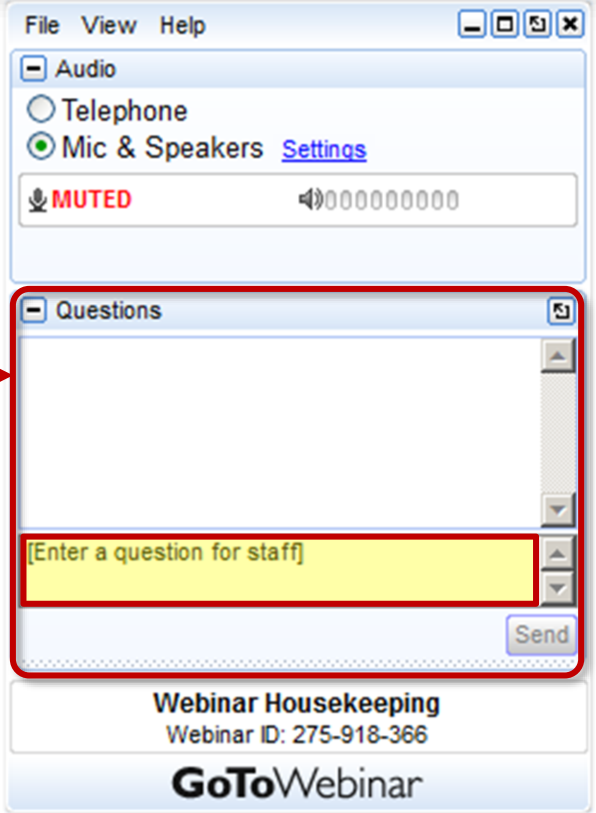
1. Fully understanding the requirements of the Phase IV CAQH CORE 470 Connectivity Rule v4.0.0
2. Having enough time and staff for implementation
3. Decision makers have not given the go ahead
4. No major challenges
5. Not applicable

Audience Q&A

Please submit your questions

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

You can also submit questions at any time to CORE@caqh.org



Reminder - Download a copy of today’s presentation slides at caqh.org/core/events

- Navigate to the Resources section for today’s event to find a PDF version of today’s presentation slides
- Also, a copy of the slides and the webinar recording will be emailed to all attendees in the next 1-2 business days

Upcoming CAQH CORE Education Sessions

Latest News and Dialogue on the Value of Healthcare e-Payments
THURSDAY, NOVEMBER 17TH, 2016 – 2 PM ET

Training Session on Annual Industry Opportunity to Make Changes to the CAQH CORE Code Combinations – The 2016 Market Based Review
THURSDAY, DECEMBER 8TH, 2016 – 2 PM ET

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

Engage With Us!

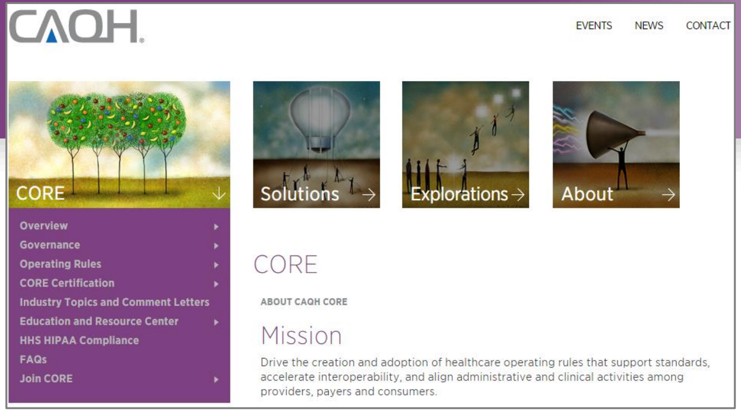
Visit us at the CAQH CORE Website or contact us at CORE@CAQH.org

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 upcoming webinars



CORE

ABOUT CAQH CORE

Mission

Drive the creation and adoption of healthcare operating rules that support standards, accelerate interoperability, and align administrative and clinical activities among providers, payers and consumers.

Dedicated webpages:

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

Thank you for joining us!

Website: www.CAQH.org/CORE

Email: CORE@CAQH.org

@CAQH

Appendix

Phase IV CAQH CORE 470 Connectivity Rule v4.0.0

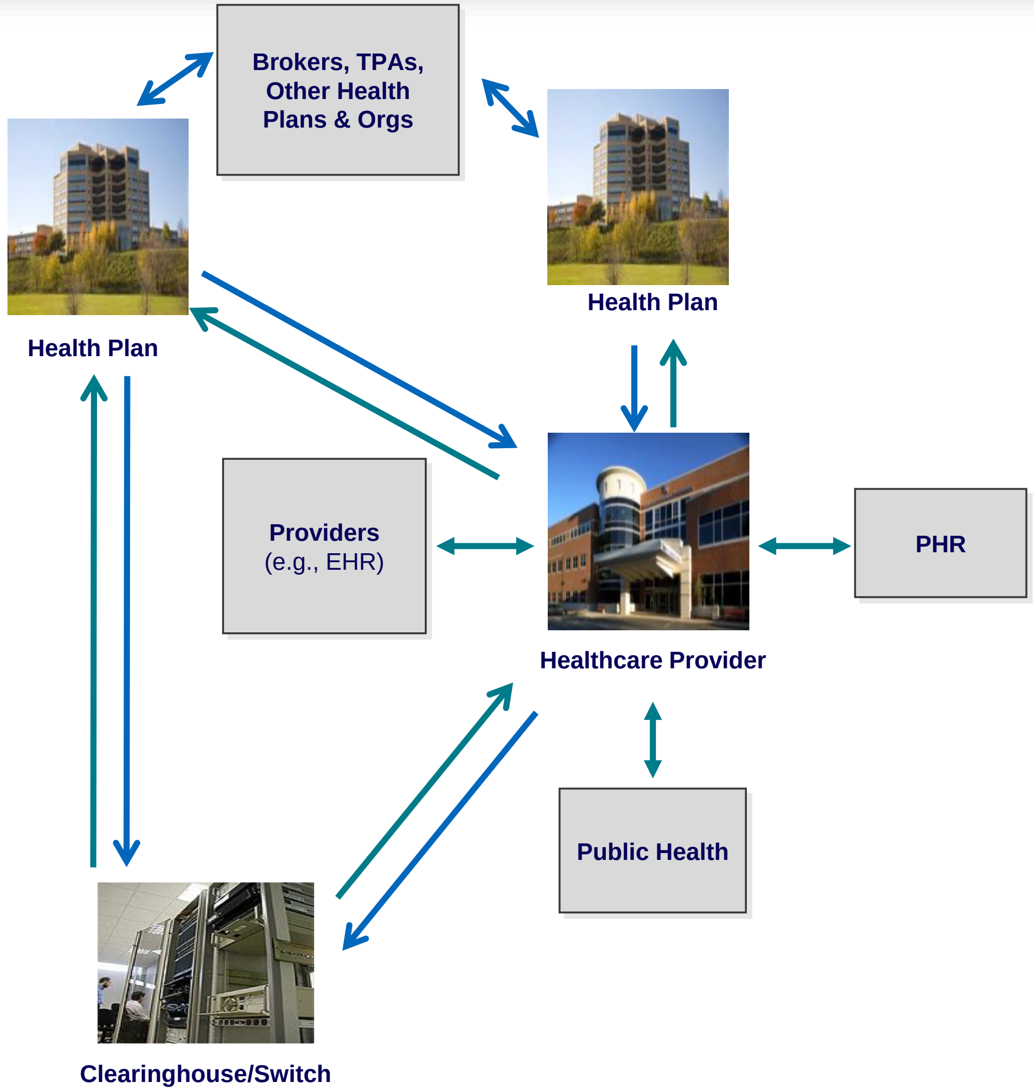
Enhancements to Electronic Transactions

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**

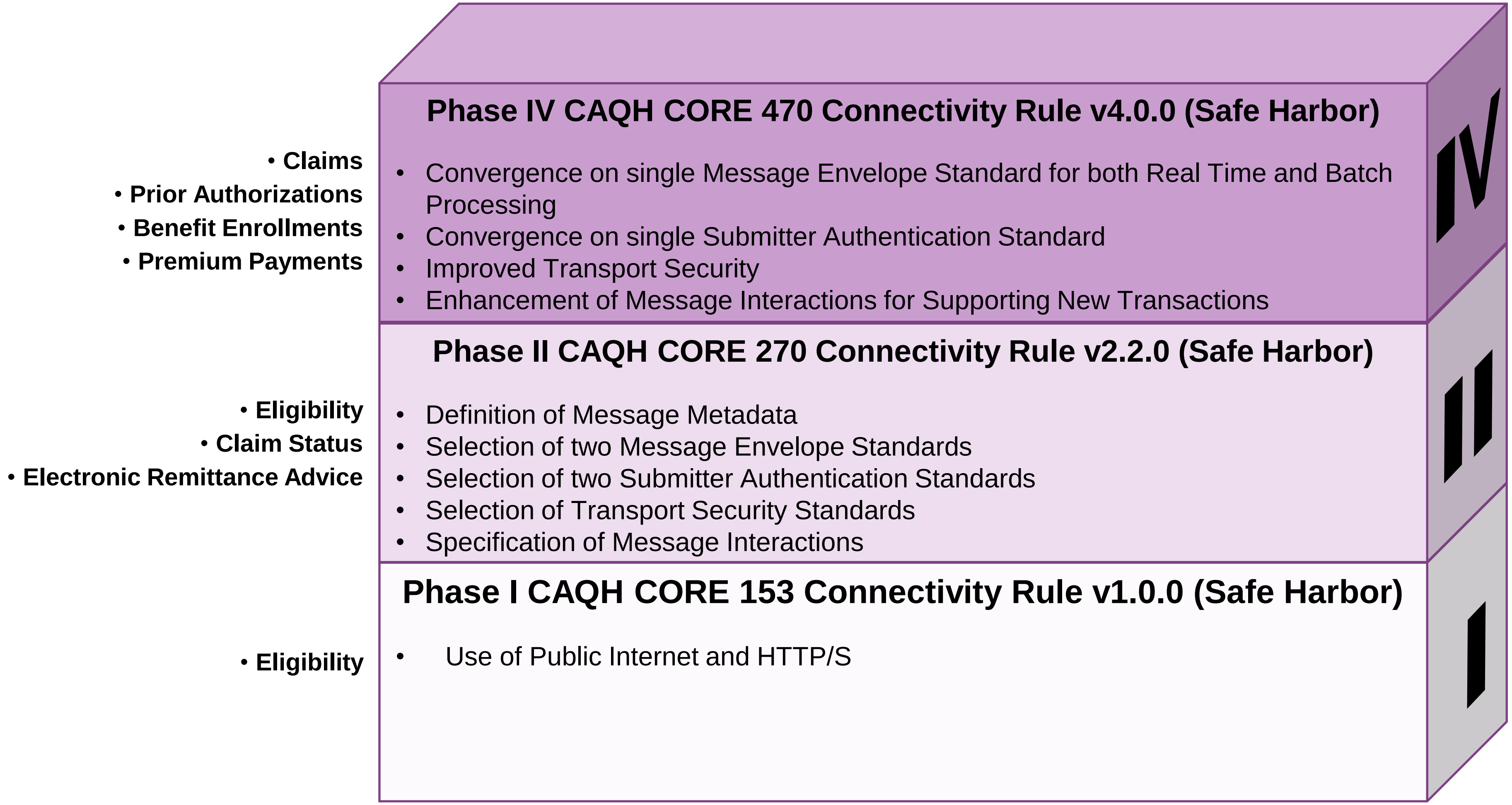
Solution: Phase IV CAQH CORE 470 Connectivity Rule v4.0.0

- ➢ **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



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

Evolution --- Each Phase Builds on Previous Phases



- Claims
- Prior Authorizations
- Benefit Enrollments
- Premium Payments

Phase IV CAQH CORE 470 Connectivity Rule v4.0.0 (Safe Harbor)

- Convergence on single Message Envelope Standard for both Real Time and Batch Processing
- Convergence on single Submitter Authentication Standard
- Improved Transport Security
- Enhancement of Message Interactions for Supporting New Transactions

- Eligibility
- Claim Status
- Electronic Remittance Advice

Phase II CAQH CORE 270 Connectivity Rule v2.2.0 (Safe Harbor)

- Definition of Message Metadata
- Selection of two Message Envelope Standards
- Selection of two Submitter Authentication Standards
- Selection of Transport Security Standards
- Specification of Message Interactions

- Eligibility

Phase I CAQH CORE 153 Connectivity Rule v1.0.0 (Safe Harbor)

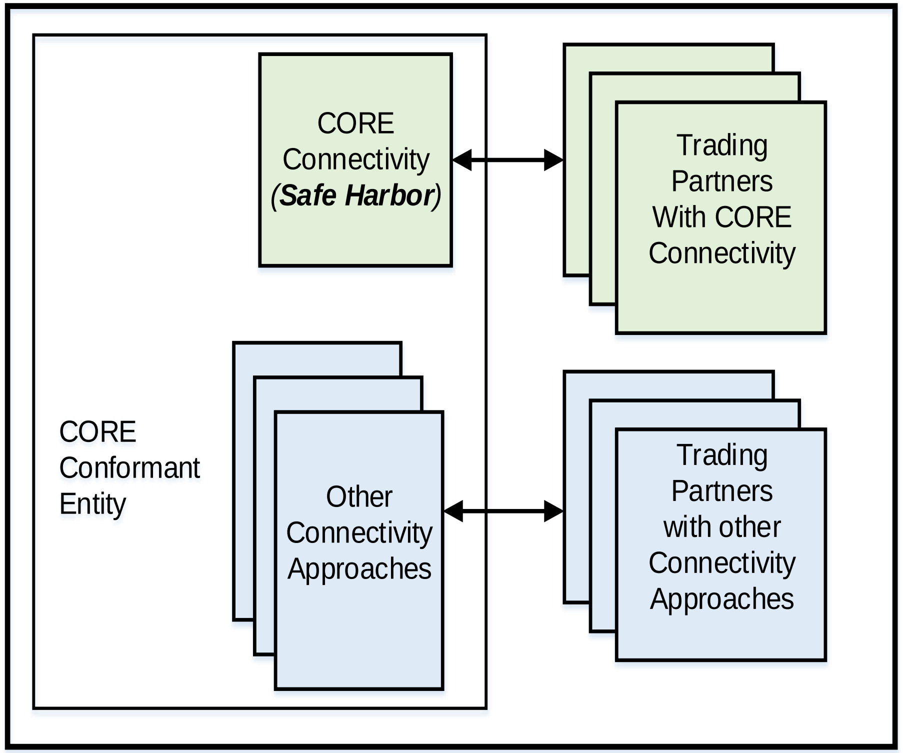
- Use of Public Internet and HTTP/S

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


CORE Connectivity (*Safe Harbor*)
Trading Partners With CORE Connectivity
CORE Conformant Entity
Other Connectivity Approaches
Trading Partners with other Connectivity Approaches

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

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

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.

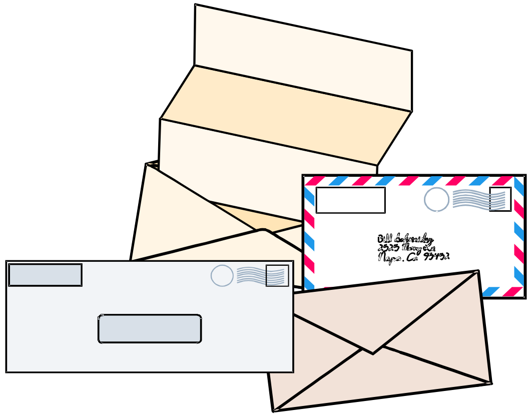
Applies to both batch and Real Time transactions. Does not require trading partners to remove existing connections that do not match the rules.

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

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:

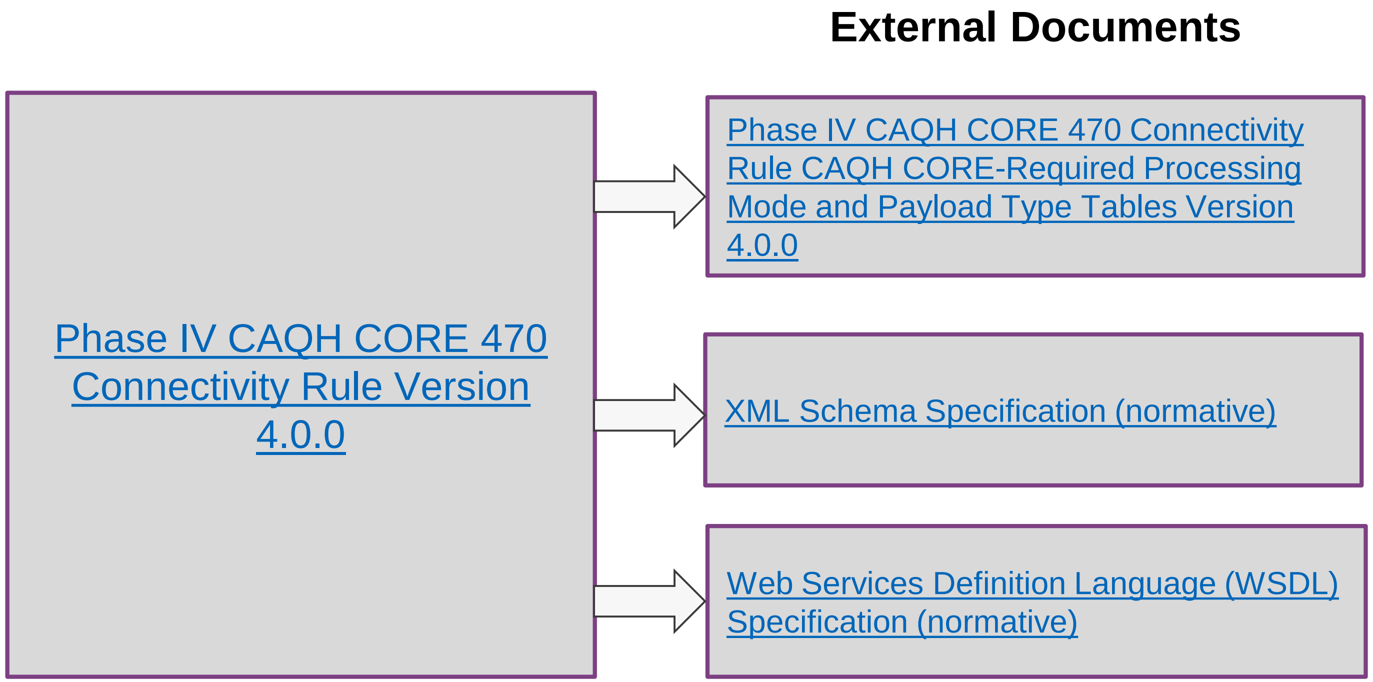
- X.509 Client Certificate based authentication over SSL/TLS is stronger than username + password
- Reduced implementation cost and complexity having one standard
- Client certificate based authentication requires the submitter to access its cryptographic key (private key) to use its public key certificate
- 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

Phase IV CAQH CORE 470 Connectivity Rule v4.0.0

External Documents



External Documents

Phase IV CAQH CORE 470 Connectivity Rule Version 4.0.0

Phase IV CAQH CORE 470 Connectivity Rule CAQH CORE-Required Processing Mode and Payload Type Tables Version 4.0.0

XML Schema Specification (normative)

Web Services Definition Language (WSDL) Specification (normative)

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

Phase IV CAQH CORE 470 Connectivity Rule v4.0.0

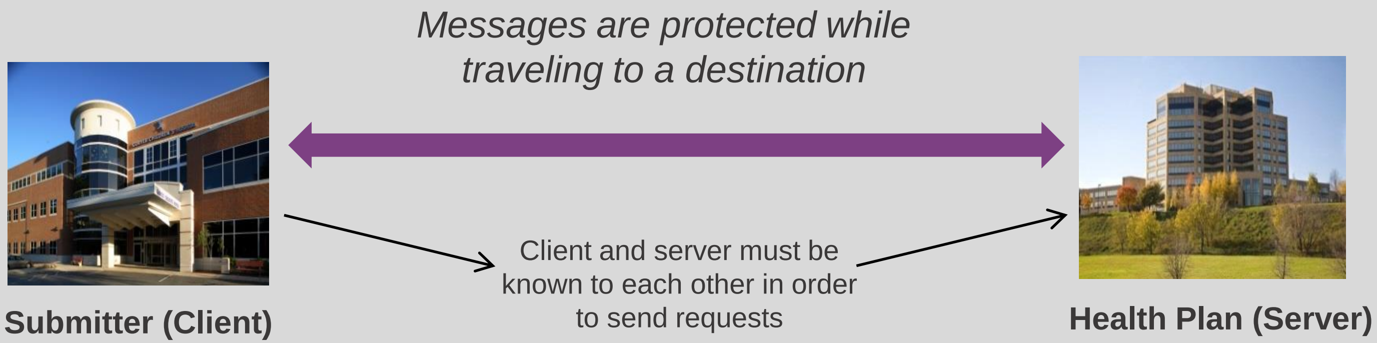
Security

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
Client and server must be known to each other in order to send requests
Submitter (Client)
Health Plan (Server)

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

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)

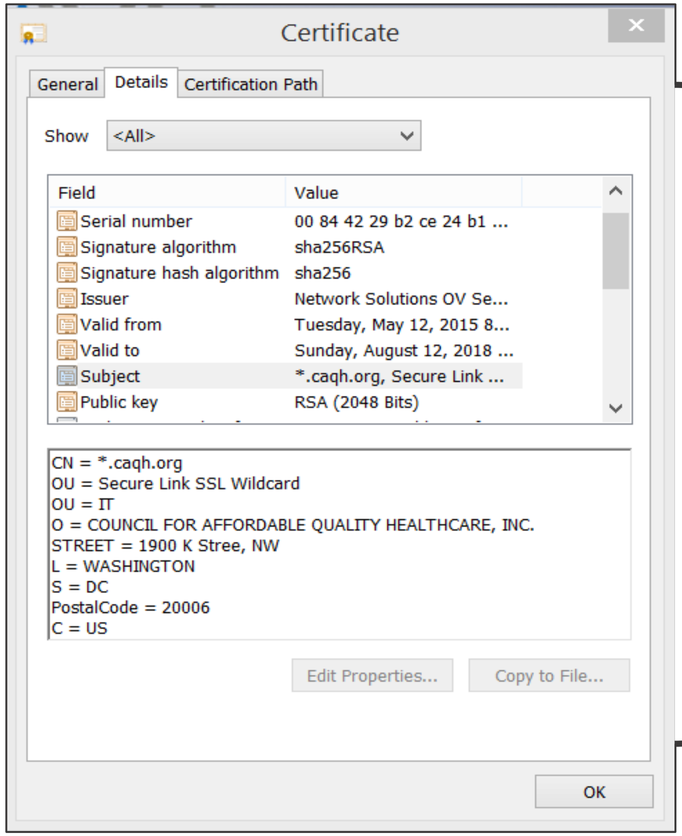
- Server certificates are installed at the Health Plan (server)
- Server certificates contain the Subject value identifying the Health Plan (server)

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 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.



Field	Value
Serial number	00 84 42 29 b2 ce 24 b1 ...
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	Network Solutions OV Se...
Valid from	Tuesday, May 12, 2015 8...
Valid to	Sunday, August 12, 2018 ...
Subject	*.caqh.org, Secure Link ...
Public key	RSA (2048 Bits)

```
CN = *.caqh.org
OU = Secure Link SSL Wildcard
OU = IT
O = COUNCIL FOR AFFORDABLE QUALITY HEALTHCARE, INC.
STREET = 1900 K Stree, NW
L = WASHINGTON
S = DC
PostalCode = 20006
C = US
```

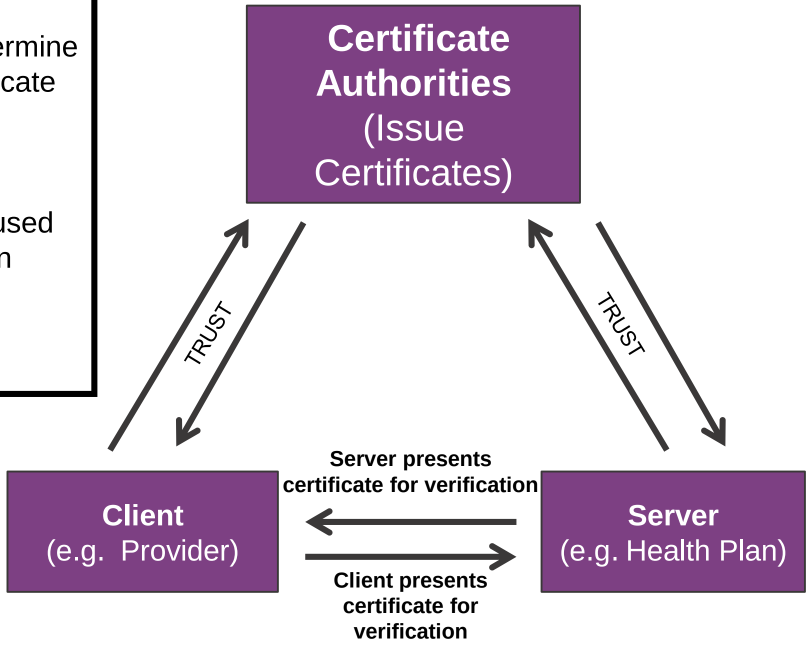
CERTIFICATE DETAILS

•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.



Certificate Authorities (Issue Certificates)

TRUST

TRUST

Client (e.g. Provider)

Server (e.g. Health Plan)

Server presents certificate for verification

Client presents certificate for verification

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

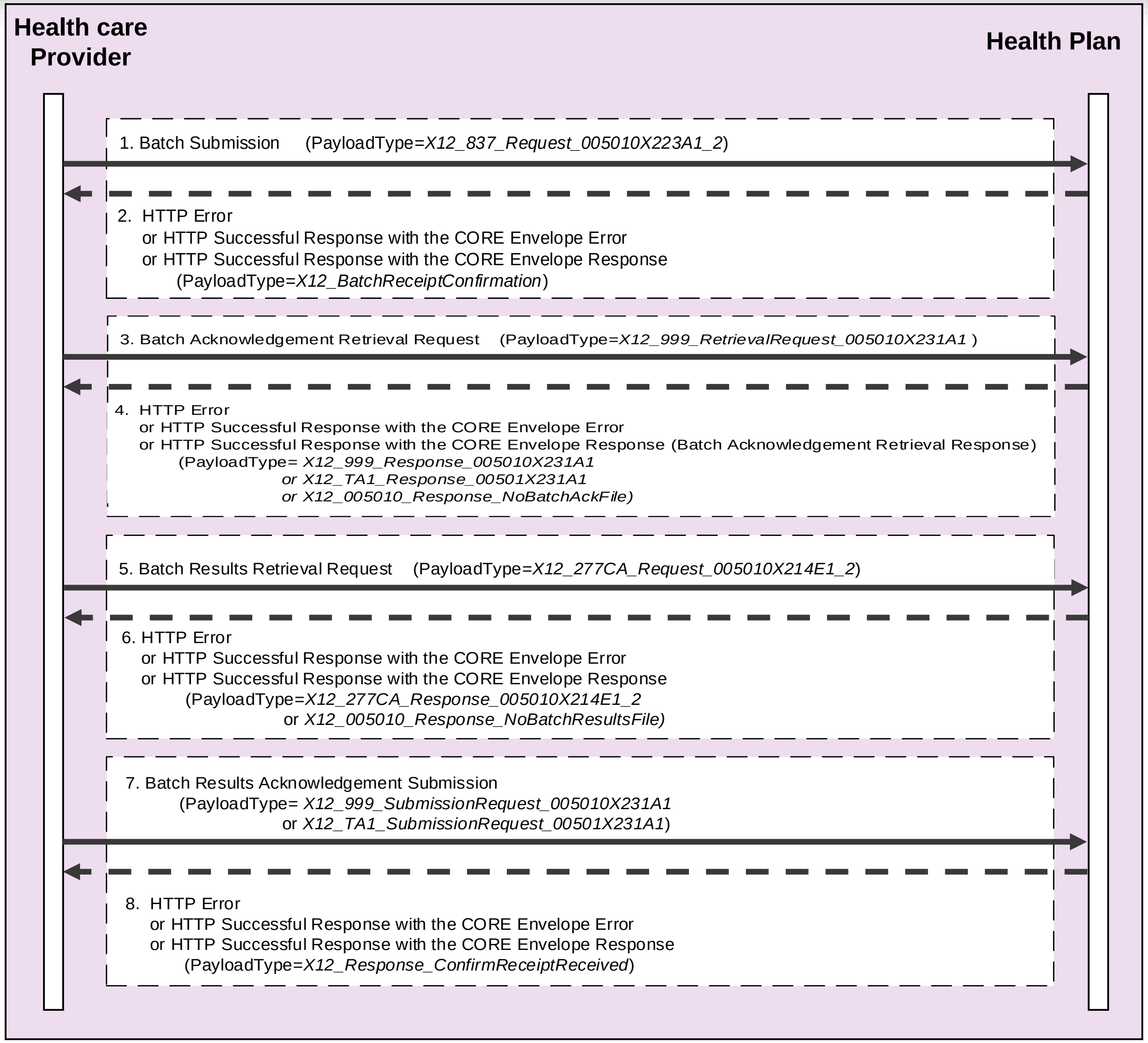
- Secure Socket Layer (SSL) Version 3.0 is a standard security technology for establishing an encrypted link between two servers
  - Provides "over the wire" (or transport level) confidentiality and integrity of the data sent over the SSL/TLS session
  - Servers are authenticated using SSL Server Certificates
  - 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 Message Interactions: *Batch Claims (ASC X12 v5010 837)* *Batch Processing Mode Example*

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.



Health care Provider

Health Plan

1. Batch Submission (PayloadType=*X12_837_Request_005010X223A1_2*)

2. HTTP Error
or HTTP Successful Response with the CORE Envelope Error
or HTTP Successful Response with the CORE Envelope Response
(PayloadType=*X12_BatchReceiptConfirmation*)

3. Batch Acknowledgement Retrieval Request (PayloadType=*X12_999_RetrievalRequest_005010X231A1*)

4. HTTP Error
or HTTP Successful Response with the CORE Envelope Error
or HTTP Successful Response with the CORE Envelope Response (Batch Acknowledgement Retrieval Response)
(PayloadType= *X12_999_Response_005010X231A1*
or X12_TA1_Response_00501X231A1
or X12_005010_Response_NoBatchAckFile)

5. Batch Results Retrieval Request (PayloadType=*X12_277CA_Request_005010X214E1_2*)

6. HTTP Error
or HTTP Successful Response with the CORE Envelope Error
or HTTP Successful Response with the CORE Envelope Response
(PayloadType=*X12_277CA_Response_005010X214E1_2*
or *X12_005010_Response_NoBatchResultsFile)*

7. Batch Results Acknowledgement Submission
(PayloadType= *X12_999_SubmissionRequest_005010X231A1*
or *X12_TA1_SubmissionRequest_00501X231A1*)

8. HTTP Error
or HTTP Successful Response with the CORE Envelope Error
or HTTP Successful Response with the CORE Envelope Response
(PayloadType=*X12_Response_ConfirmReceiptReceived*)

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.

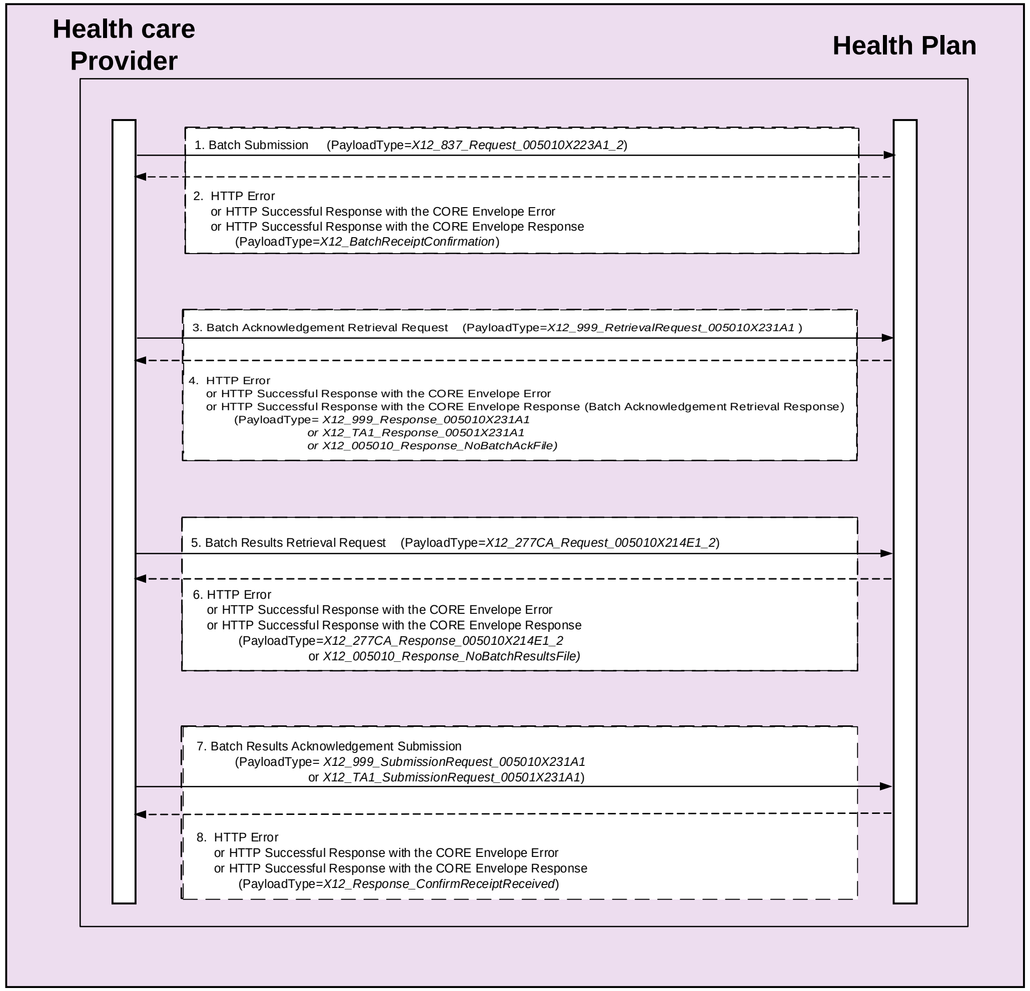
6. Health Plan responds with the ASC X12N v5010 277 Claim Acknowledgement.

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.

Phase IV CAQH CORE 470 Connectivity Rule v4.0.0 Message Interactions:

Batch Claims (ASC X12 v5010 837) Batch Processing Mode Example



1. Batch Submission (PayloadType=*X12_837_Request_005010X223A1_2*)

2. HTTP Error
   or HTTP Successful Response with the CORE Envelope Error
   or HTTP Successful Response with the CORE Envelope Response
   (PayloadType=*X12_BatchReceiptConfirmation*)

3. Batch Acknowledgement Retrieval Request (PayloadType=*X12_999_RetrievalRequest_005010X231A1*)

4. HTTP Error
   or HTTP Successful Response with the CORE Envelope Error
   or HTTP Successful Response with the CORE Envelope Response (Batch Acknowledgement Retrieval Response)
   (PayloadType= *X12_999_Response_005010X231A1*
   or X12_TA1_Response_00501X231A1
   or X12_005010_Response_NoBatchAckFile)

5. Batch Results Retrieval Request (PayloadType=*X12_277CA_Request_005010X214E1_2*)

6. HTTP Error
   or HTTP Successful Response with the CORE Envelope Error
   or HTTP Successful Response with the CORE Envelope Response
   (PayloadType=*X12_277CA_Response_005010X214E1_2*
   or *X12_005010_Response_NoBatchResultsFile)*

7. Batch Results Acknowledgement Submission
   (PayloadType= *X12_999_SubmissionRequest_005010X231A1*
   or *X12_TA1_SubmissionRequest_00501X231A1*)

8. HTTP Error
   or HTTP Successful Response with the CORE Envelope Error
   or HTTP Successful Response with the CORE Envelope Response
   (PayloadType=*X12_Response_ConfirmReceiptReceived*)

Phase IV CAQH CORE 470 Connectivity Rule v4.0.0

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