Committee on Operating Rules For Information Exchange (CORE®)

Just the Facts: A Technical Presentation with Q&A on Federally Mandated CAQH CORE Connectivity Rules and Requirements for ACA Section 1104

October 17, 2012
2:00 pm – 3:30 pm ET

Erin Richter
CORE Senior Manager
CAQH

Raja Kailar
Chief Executive Officer
Business Networks International, Inc. (BNETAL)

Kevin Castellow
Senior Consultant
BNETAL

This document is for educational purposes only; in the case of a question between this document and CAQH CORE Operating Rule text and/or Federal regulations, the latter take precedence.
Overview

• Purpose
  – This presentation will provide technical details and review the requirements for implementing the federally mandated CAQH CORE Operating Rules with a focus on those rules related to connectivity

• Audience
  – The intended audience consists of technical implementers of CAQH CORE Connectivity Rules for Eligibility and Claim Status Transactions in your organization

• Prerequisites
  – Basic understanding of CAQH CORE mission, vision and Guiding Principles; please click HERE for an overview
  – Conceptual understanding of Connectivity Rules that are part of the federally mandated Operating Rules set. CAQH CORE general background information is available by clicking HERE
  – Working knowledge of technical concepts such as client/server connectivity and Message Envelope Protocols including SOAP+WSDL or HTTP+MIME multipart

• Required Materials
  – This PowerPoint and a copy of the CAQH CORE Connectivity Operating Rules for reference
  • Phase I Connectivity click HERE
  • Phase II Connectivity click HERE
Presentation Outline

• Technical Concepts: Mandated CAQH CORE Connectivity Operating Rules
  – Safe Harbor Principle
  – Message Envelope Standards
  – Payload Processing Modes and Messaging Interaction Types

• Technical Requirements: Mandated CAQH CORE Connectivity Operating Rules
  – Envelope Requirements
  – Security Requirements
  – Payload Processing Mode Requirements
  – Conformance Requirements for Stakeholders
  – Requirements based on other CAQH CORE Infrastructure Operating Rules

• Q&A/Commonly Asked Questions

• CAQH CORE Resources for Implementers
### Federally Mandated CAQH CORE Connectivity Rules:

**Requirements Scope for HIPAA Covered Entities**

The focus of the presentation is on **Connectivity Rules**

<table>
<thead>
<tr>
<th>Rule Types</th>
<th>Transactions</th>
<th>Rule Areas</th>
<th>CAQH CORE Rule Numbers</th>
<th>Key Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Infrastructure</td>
<td>X12 270/271 Eligibility &amp; Benefits and X12 276/277 Claims Status</td>
<td>Response Time Rules (Batch &amp; Real-Time) &amp; System Availability Rule</td>
<td>155, 156, 157, &amp; 250*</td>
<td>Interdependencies of the CAQH CORE Infrastructure Rules must be considered during implementation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Connectivity Rules</td>
<td>153, 270 &amp; 250*</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Companion Guide Rule</td>
<td>152 &amp; 250*</td>
<td></td>
</tr>
<tr>
<td>Data Content</td>
<td>X12 270/271 Eligibility &amp; Benefits</td>
<td>Patient Financial Data Content Rules</td>
<td>154 &amp; 260</td>
<td>Data Content Rules apply only to the Eligibility &amp; Benefits transaction</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Normalizing Patient Last Name &amp; AAA Error Code Reporting Rules</td>
<td>258 &amp; 259</td>
<td></td>
</tr>
</tbody>
</table>

*CAQH CORE Rule 250 applies the CAQH CORE Infrastructure Rules to the X12 276/277 Claims Status transaction.
Federally Mandated CAQH CORE Connectivity Rules

• Problem addressed by rules
  – Multiple methods for exchanging eligibility and benefits data both manually and/or electronically drive elevated transaction costs and increase operational complexity

• Scope of the rules
  – Using the internet as a delivery option, establishes a “Safe Harbor” connectivity rule which standardizes the flow of administrative transactions between health plan and provider
    • Rule 270 builds on Rule 153 to include more prescriptive submitter authentication, envelope specifications, etc.
    • Safe Harbor applies when an entity uses, conducts or processes the X12 270/271 Eligibility & Benefits and X12 276/277 Claim Status transactions
      – Applies to information sources performing the role of an HTTP/S server and information receivers performing the role of an 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
Federally Mandated CAQH CORE Infrastructure Rules

- **Connectivity Rules**
  - Clients and servers must follow requirements in the CAQH CORE Connectivity Rules: CAQH CORE Rules 270 and 153

- **Response Time Rules**
  - Servers must follow the requirements for response times for Real time interactions in CAQH CORE Real time Response Time Rule: CAQH CORE Rule 156
  - Servers must follow the requirements for response times for Batch interactions as stated in CAQH CORE Batch Response Rule: CAQH CORE Rule 155

- **System Availability Rule**
  - Servers must follow the requirements for system availability requirements in CAQH CORE System Availability Rule: CAQH CORE Rule 157

- **Companion Guide Requirement**
  - Servers must publish detailed specifications in a Connectivity Companion Guide; the guide should be consistent with the guidelines for companion guides described in the CAQH CORE Connectivity Rule 270
  - CAQH CORE makes recommendations in CAQH CORE Connectivity Rule 270 for specific topics and information in the Companion Guide

**NOTE:** Many of the Federally mandated CAQH CORE Infrastructure Rules also apply to the ASC X12 v5010 835 per CMS-0028-IFC.
Federally Mandated CAQH CORE Connectivity Rules: Multi-stakeholder Connectivity

- When a clearinghouse or vendor is involved in data exchange between the health plan and the provider’s eligibility systems, then:
  - Identifying the role and responsibility of each entity from an end-to-end perspective is an important step
  - Each entity will be responsible for their own specific implementation, testing and related resources
  - Joint integration planning between HIPAA covered entities and their vendors will ensure that conformance requirements and return on investment (ROI) goals are met

- CAQH CORE Connectivity Rules are a set of requirements that represent a minimum level of requirements
  - Entities may go above and beyond the rules to ensure the implementations meet their needs
Federally Mandated CAQH CORE Connectivity Rules: Connected Systems and Applicable Architectures

- Interoperability and efficiency is enhanced by the rules defined technical requirements for exchange of administrative transactions between trading partners
  - Connectivity Rules can be applied independent of the communication architecture or model (e.g., two models are shown below)
  - Connectivity Rules do not apply to Direct Data Entry (DDE) systems

**Model 1: Direct Connectivity**
- Provider
- Health Plan

**Model 2: Connectivity with Intermediary**
- Provider
- Health Plan
- Clearinghouse
Federally Mandated CAQH CORE Connectivity Rules: Message Interactions

Description of CAQH CORE Connectivity Rules Using a Direct (i.e., with no intermediaries) Connectivity Example

CAQH CORE Connectivity Rules apply to the message interactions between connected systems

- CAQH CORE Connectivity Rules are a set of operating rules that describe on an operational level how the systems should interact
- The rules contain details that include the message format, the response times, authentication methods, and responsibilities based on roles of the senders and receivers
- CAQH CORE Connectivity Rules set a minimum level of security; designed to protect the information and communication channels; entities may implement additional security measures
Federally Mandated CAQH CORE Connectivity Rules: Security

Description of CAQH CORE Connectivity Rules with Direct (i.e., with no intermediaries) Connectivity Example

Messages are protected while traveling to destination

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

Provider (Client)  Health Plan (Server)

• The security aspects of CAQH CORE Connectivity Rules are intended to ensure:
  – A message is not tampered with while traveling to partner systems
  – The message came from a known partner

Note: CAQH CORE Connectivity Rules are a Base, not a Ceiling.
Federally Mandated CAQH CORE Connectivity Rules: Layered View

**Application Layer:**
- CAQH CORE Connectivity Rules are “Payload Agnostic”, hence do not specify the Application file or processing layer

**Message Encapsulation Layer:**
- CAQH CORE Connectivity Rules define a prescriptive Message Envelope structure and metadata

**Message Transport Layer:**
- Both CAQH CORE Connectivity Rules 153 and 270 prescribe use of a securely encrypted Message Transport Layer
  - Both require HTTP over SSL; CAQH CORE Rule 270 includes optional use of TLS
Federally Mandated CAQH CORE Connectivity Rules: Safe Harbor Principle

- The connectivity requirements that a trading partner must use if requested by another trading partner are described in the CAQH CORE Connectivity Rules as the CORE Connectivity Safe Harbor.

- **CAQH CORE Rule 270** Section 5, *CORE Safe Harbor*, defines the CAQH CORE Connectivity Safe Harbor:
  - The CAQH CORE Connectivity Safe Harbor specifies connectivity methods that application vendors, providers, and health plans can be assured will be supported by any HIPAA covered entity, meaning that the entity is capable and ready at the time of the request by a trading partner to exchange data using the CAQH CORE Connectivity Rule.
  - The rule does not require entities to remove existing connections that do not match the rule, nor does it require that all covered entities use this method for all new connections. In some circumstances, you and your trading partners may decide to continue to use your current connection; however you must implement the capability to use the CORE Connectivity Safe Harbor when requested.
Federally Mandated CAQH CORE Connectivity Rules: Message Envelope Standards

- CAQH CORE Connectivity Rules support two envelope standards (subject to basic conformance requirements)
  - CAQH CORE Connectivity Rule 270 selected HTTP MIME Multipart and SOAP + WSDL as the two standards that met the majority of CAQH CORE technical criteria and had wide industry use
  - CAQH CORE Connectivity Rule 270 specifies a SOAP envelope structure using XSD schemas and HTTP MIME envelope using examples

**Envelope Standard A: HTTP MIME Multipart**
- Multipart envelope that is based on MIME standard (non-XML)
- MIME structure supports sending CAQH CORE Connectivity Rule metadata and payload
- Does not provide schemas for envelope

**Envelope Standard B: SOAP 1.2**
- SOAP+WSDL messaging
- Structured envelope that contains CAQH CORE Connectivity Rule metadata and Payload (e.g., using MTOM)
- WSDL and XSD (schema) files are provided files that allow for automated verification
Federally Mandated CAQH CORE Connectivity Rules: Payload Processing Modes/Interactions

- **CAQH CORE Connectivity Rules address both Real time & Batch payload processing modes**
- **Payload Processing Modes describe how message payload is processed**

<table>
<thead>
<tr>
<th>Processing Modes</th>
<th>Description</th>
</tr>
</thead>
</table>
| Real time        | • Entity sends single request, receives single response in Real time  
                  • Servers must follow the requirements for response times for Real time interactions in CAQH CORE Real time Response Rule: [CORE Rule 156](#)  
| Batch            | • Entity submits Batch of requests at the same time  
                  • Results of processing the Batch of requests are sent back at a later time (i.e., not in Real time)  
                  • Batch (asynchronous) processing is optional for X12 v5010 270/271 and X12 v5010 276/277 transactions |
Federally Mandated CAQH CORE Connectivity Rules: Payload Processing Modes and Messaging Interactions

**CAQH CORE Connectivity Rule 270 addresses synchronous & asynchronous message interaction pattern:** Message Interaction Patterns describe how connections are established and used for handling requests and responses.

<table>
<thead>
<tr>
<th>Message Interaction Patterns</th>
<th>Description</th>
</tr>
</thead>
</table>
| **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 Real time mode of processing |
| **Asynchronous**            | • Connection is established to send a request; response is sent on a separate connection  
• Typically associated with Batch mode of processing |

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

- Provider (Client)
- Health Plan (Server)

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

- Provider (Client)
- Health Plan (Server)
  - Session 1
  - Session 2
Are You Ready for Trading Partner Testing?

- Testing with your trading partners is a critical aspect to making your operating rules implementation a success, as well as that of those entities with which you exchange HIPAA transactions.

- Given the Federal deadline for the 1\textsuperscript{st} set of operating rules is January 1, 2013, CAQH CORE is now hosting a website to highlight those organizations in trading partner testing.

- HIPAA covered entities (or other key IT systems that support them, such as Practice Management Systems) can quickly list that their organization is ready to test with its trading partners.
  - Those entities using the website that are voluntarily CORE-certified have their CORE Certification Seal listed, given such entities already are using the CORE rules in daily exchange and thus able to test with their trading partners.

- The website can be found at \url{http://caqh.org/COREPartnerTesting.php}

\textit{If you are ready, add your organization today!}
Technical Requirements of Mandated CAQH CORE Connectivity Operating Rules

There will be Time for Q & A at the End of the Presentation
# Federally Mandated CAQH CORE Connectivity Rules:
## High Level Rule Requirements

<table>
<thead>
<tr>
<th>CAQH CORE Connectivity Rule Area</th>
<th>CAQH CORE Connectivity Rules</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>Internet</td>
</tr>
<tr>
<td>Transport</td>
<td>HTTP</td>
</tr>
<tr>
<td>Transport Security</td>
<td>SSL, TLS (optional)</td>
</tr>
</tbody>
</table>
| Submitter (Originating System or Client) Authentication | Name/Password  
X.509 Certificate (subject to conformance requirements) |
| Envelope and Attachment Standards | SOAP 1.2 + WSDL and MTOM (for Batch) or  
HTTP+MIME (subject to conformance requirements) |
| Envelope Metadata                | Metadata defined (Field names, values)  
New PayloadTypes for HIPAA and non-HIPAA Payloads |
| Message Interactions/            | Real time                    |
| Routing                          | Batch (Optional if used)     |
| Acknowledgements, Errors         | Specified                    |
| Basic Conformance Requirements   | Specified                    |
| Response Time                    | Specified                    |
| System Availability              | Specified                    |
| Companion Implementation Guide   | Specified                    |
Federally Mandated CAQH CORE Connectivity Rules: *Message Structure*

- CAQH CORE Connectivity Rule 270 metadata is prescriptive to facilitate interoperability of administrative transactions

  - Public Internet (TCP/IP) – CORE Connectivity Rule 153
  - HTTP over SSL (HTTP/S) – CORE Connectivity Rule 153 (includes security of payload during transmission)
  - Message Envelope & Message Metadata – CORE Connectivity Rule 270 Rule (independent of payload – required by CORE Connectivity Rule 153)
  - HIPAA Administrative Transactions (X12)
    - HL7 Clinical Messages
    - Zipped Files
    - Personal Health Record
    - Other Content
Federally Mandated CAQH CORE Connectivity Rules: Side-by-Side Comparison of Envelopes

SOAP Envelope

POST /core/eligibility HTTP/1.1
Host: server_host:server_port
Content-Type: application/soap+xml; charset=UTF-8; action="RealTimeTransaction"

<soapenv:Envelope
xmlns:soapenv="http://www.w3.org/2003/05/soap-envelope">
<soapenv:Header>
<wsse:Security
xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" soapenv:mustUnderstand="true">
<wsse:UsernameToken xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" wsu:Id="UsernameToken-21621663">
<wsse:Username>bob</wsse:Username>
<wsse:Password Type="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">bobPW</wsse:Password>
</wsse:UsernameToken>
</wsse:Security>
</soapenv:Header>
<soapenv:Body>
<ns1:COREEnvelopeRealTimeRequest
xmlns:ns1="http://www.caqh.org/SOAP/WSDL/CORERule2.2.0.xsd">
<PayloadType>X12_270_Request_005010X279A1/PayloadType>
<ProcessingMode>RealTime</ProcessingMode>
<PayloadID>e51d4fae-7dec-11d0-a765-00a0c91e6da6</PayloadID>
<TimeStamp>2007-08-30T10:20:34Z</TimeStamp>
<SenderID>HospitalA</SenderID>
<ReceiverID>PayerB</ReceiverID>
</ns1:COREEnvelopeRealTimeRequest>
</soapenv:Body>
</soapenv:Envelope>

HTTP Headers (Both Messages)

POST /core/eligibility HTTP/1.1
Host: server_host:server_port
Content-Type: multipart/form-data; boundary=XbCY

--XbCY
Content-Disposition: form-data; name="PayloadType"
X12_270_Request_005010X279A1
--XbCY
Content-Disposition: form-data; name="ProcessingMode"
RealTime
--XbCY
Content-Disposition: form-data; name="PayloadID"
e51d4fae-7dec-11d0-a765-00a0c91e6da6
--XbCY
Content-Disposition: form-data; name="TimeStamp"
2007-08-30T10:20:34Z
--XbCY
Content-Disposition: form-data; name="UserName"
hospa
--XbCY
Content-Disposition: form-data; name="Password"
e51d4fae-7dec-11d0-a765-00a0c91e6da6
--XbCY
Content-Disposition: form-data; name="SenderID"
HospitalA
--XbCY
Content-Disposition: form-data; name="ReceiverID"
PayerB
--XbCY
Content-Disposition: form-data; name="CORERuleVersion"
2.1.0
--XbCY
Content-Disposition: form-data; name="Payload"
filename="name.txt"

<contents of file go here -- 1674 bytes long as specified above>
--XbCY--
Federally Mandated CAQH CORE Connectivity Rules: Security Across the Layers

- Transport Security: Security (e.g., authentication, integrity) for electronic transactions conducted over common medium of access
- CAQH CORE Connectivity Rules’ security requirements:
  - Secure Socket Layer (SSL) 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 3.0 (and optionally TLS) for transport level security
    - Does not preclude optional use of TLS 1.0 (or higher version as required for FIPS 140 compliance) for connectivity with trading partners that require FIPS 140 compliance
  - For authenticating clients (i.e., “Submitters”), one of two approaches is used:
    - X.509 Certificates over SSL (optionally, over TLS)
    - Username and Password (e.g., WS-Security Username Token in the SOAP option)
  - For payload integrity verification:
    - SHA-1 Checksum of the payload is sent as part of the message envelope
  - For reliability of transport:
    - UUID is used for Payload ID (for detecting duplicates)
    - Timestamp is used for ensuring that the data is recent

Note: CAQH CORE Connectivity Rules are a base, not a ceiling
Federally Mandated CAQH CORE Connectivity Rules: 
**Payload Processing Modes**

- **Real time Payload Processing Requirements:**
  - Requires Real time (synchronous) processing for X12 v5010 270/271 and X12 v5010 276/277 transactions
  - Diagram illustrates Real time (synchronous) interaction between a provider and health plan

  ![Diagram](image)

  - **Message Sequence 1:** Provider submits Real time request to health plan using payload type as X12_270_Request_005010X279A1 or one of the specific payload types
  - **Message Sequence 2:** Health plan responds (synchronously to message 1) with HTTP level error or HTTP successful response accompanied by CORE Envelope Level response (Payload type is X12_271_Response_005010X279A1 or error)
Federally Mandated CAQH CORE Connectivity Rules: Payload Processing Modes (cont’d)

• Batch Payload Processing Requirements:
  – Batch (asynchronous) processing is optional for X12 v5010 270/271 and X12 v5010 276/277 transactions
  – However, if an entity performs Batch processing for X12 v5010 270/271 and X12 v5010 276/277, it must conform to the Batch processing specifications for X12 v5010 270/271 and X12 v5010 276/277 transactions
  – There are a few defined interactions for Batch processing within CAQH CORE Connectivity Rule 270:
    • Interaction can be conducted using specific or mixed payload types
    • Generic Batch retrieval request and receipt confirmation
    • Generic Batch submission with Batch payload and synchronous payload receipt confirmation
### Federally Mandated CAQH CORE Connectivity Rules: Error Handling

**CAQH CORE Connectivity Rules address errors that can be returned at each logical layer**

<table>
<thead>
<tr>
<th>Error Type</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>HTTP Status and Error Codes</strong></td>
<td>Rely upon the IETF RFC 2616 for the specific and complete list of protocol specific errors that must be supported&lt;br&gt;CAQH CORE Connectivity Rules (153 and 270) describe transport level status and error conditions and the use of HTTP status and error codes for those conditions</td>
</tr>
<tr>
<td><strong>Envelope Processing Status and Error Codes</strong></td>
<td>Errors while processing the envelope (e.g., rule version mismatch)&lt;br&gt;Error codes are enumerated in CAQH CORE Connectivity Rule 270&lt;br&gt;The intended use is defined in the rule documentation</td>
</tr>
<tr>
<td><strong>Payload Processing Error Messages</strong></td>
<td>Payload (e.g., ASC X12) processing status (e.g., ASC X12 999) or errors (e.g., ASC X12 TA1) are the responsibility of the application&lt;br&gt;The HHS <a href="https://www.hhs.gov/ocr/privacy/hipaa/administrative/finalrules/eligibility/index.html">Final Rule for Administrative Simplification: Adoption of Operating Rules for Eligibility for a Health Plan and Health Care Claim Status Transaction</a>, requirements pertaining to use of Acknowledgements are NOT included for adoption. Although HHS is not requiring compliance with any operating rule requirements related to Acknowledgements, the Final Rule does note “we are addressing the important role acknowledgements play in EDI by strongly encouraging the industry to implement the acknowledgement requirements in the CAQH CORE rules we are adopting herein.”</td>
</tr>
</tbody>
</table>
Federally Mandated CAQH CORE Connectivity Rules: 

**Error Handling**

- Once request (e.g., X12 270) is submitted, it goes through **3 logical layers**:  
  - Processing of HTTP headers (typically handled by a web-server)
  - Processing the Envelope (can be handled by messaging middle-ware or integration brokers)
  - Processing the Payload (e.g., ASC X12, typically handled by application business logic)

- At each layer, some part of request is processed and errors can be returned to submitter  
  - If there is an error in processing message at any layer, request is not passed to the next layer  
  - If no errors are encountered, request is passed to the next processing layer  
  - Last logical layer that processes request is the Payload Processing Layer  
  - Once payload is processed at Payload Processing Layer, it returns a response or error
Federally Mandated CAQH CORE Connectivity Rules: Stakeholder Conformance Guidelines

- CAQH CORE Connectivity Rules apply to health plans (HTTP/S server) and health care providers (HTTP/S client)
  - The rules define conformance requirements for stakeholders based on typical role (client, server) for envelope and authentication standards
  - Diagram illustrates the typical (minimal) roles played by stakeholders (e.g., providers typically clients, health plans typically servers, clearinghouses can act as client or server)

<table>
<thead>
<tr>
<th>If your organization is a:</th>
<th>then your minimum technical role is a:</th>
<th>and CAQH CORE defines technical requirements for</th>
</tr>
</thead>
<tbody>
<tr>
<td>Healthcare Provider</td>
<td>Client</td>
<td>Client Conformance Requirements</td>
</tr>
<tr>
<td>Clearinghouse/Switch</td>
<td>Client and Server</td>
<td>Client Conformance Requirements Server Conformance Requirements</td>
</tr>
<tr>
<td>Health Plan</td>
<td>Server</td>
<td>Server Conformance Requirements</td>
</tr>
</tbody>
</table>
Federally Mandated CAQH CORE Connectivity Rules: Envelope Standards

- Stakeholders in server role (e.g., health plans and clearinghouses/switches) must implement both envelope standards (SOAP+WSDL and HTTP MIME Multipart)
- Stakeholders in client role (e.g., healthcare providers or provider vendors) must implement one of the envelope standards

If your organization is a:

- **Health Plan**
  - Server Conformance Requirements
- **Clearinghouse/Switch**
  - then you must implement both of these envelope standards
  - HTTP Multipart MIME
  - SOAP
- **Healthcare Provider**
  - Client Conformance Requirements
  - then you must implement one of these envelope standards
  - HTTP Multipart MIME
  - SOAP
Federally Mandated CAQH CORE Connectivity Rules: 
Submitter Authentication

- CAQH CORE Connectivity Rules support two methods for Submitter Authentication:
  - Username/Password, using CORE-conformant Envelope to send CORE-conformant Envelope Metadata UserName and Password
  - X.509 Certificate based authentication over SSL standard for client certificate based authentication

- Stakeholders in server role (e.g., health plans) choose to implement one of the standards
- Stakeholders in client role (e.g., healthcare providers/provider vendors and clearinghouse components handling submissions to plans) must implement both standards

If your organization is a:

<table>
<thead>
<tr>
<th>Health Plan</th>
<th>Clearinghouse/Switch</th>
<th>Healthcare Provider</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Conformance Requirements</td>
<td>then implement <strong>one</strong> of these authentication standards</td>
<td>then you must implement <strong>both</strong> of these authentication standards</td>
</tr>
<tr>
<td>Username/Password</td>
<td>X. 509 Certificate over SSL</td>
<td>Username/Password</td>
</tr>
</tbody>
</table>
30-Minute Q & A: 
Technical Questions on Mandated CAQH CORE Connectivity Rules

Your feedback will help us with new CAQH CORE reference materials
### Questions

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Real time: Is this required? Can you tell me definitively? Do we have to implement Real time even if none of our trading partners are asking for it?</td>
</tr>
<tr>
<td>2.</td>
<td>Do we have to implement or can we offer Batch over our FTP?</td>
</tr>
<tr>
<td>3.</td>
<td>If a health plan only accepts transactions from its clearinghouse, must the health plan also implement CAQH CORE connectivity, or can the health plan delegate that responsibility to the clearinghouse?</td>
</tr>
<tr>
<td>4.</td>
<td>How is downtime defined/ measured?</td>
</tr>
<tr>
<td>5.</td>
<td>How is the 20 second response time measured?</td>
</tr>
<tr>
<td>6.</td>
<td>What data do I have to track/audit? Do I have to deliver this data to anyone?</td>
</tr>
<tr>
<td>7.</td>
<td>What are the minimum interactions that must be supported for compliance with the CAQH CORE 270 Connectivity Rule?</td>
</tr>
<tr>
<td>8.</td>
<td>How does the CORE Companion Guide Rules 152 and 250, which require the use of the CAQH CORE Master Companion Guide Template, relate to the CORE Connectivity Rule which requires a Server-Specific Connectivity Guide?</td>
</tr>
<tr>
<td>9.</td>
<td>OTHER</td>
</tr>
<tr>
<td></td>
<td>1. Please submit your questions during this presentation to the <strong>Q&amp;A</strong></td>
</tr>
<tr>
<td></td>
<td>2. After the presentation submit your questions to <a href="mailto:CORE@caqh.org">CORE@caqh.org</a></td>
</tr>
</tbody>
</table>