Committee on Operating Rules For Information Exchange (CORE®)

Federally Mandated CAQH CORE Infrastructure Operating Rules for Eligibility and Claim Status Transactions

December 7, 2012
2:00 pm – 3:30 pm ET

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.
Participating in Today’s Interactive Event

• Download a copy of today’s presentation
• The phones will be muted upon entry and during the presentation portion of the session
• At any time throughout today’s session, you may communicate with our panelists via the web
  – Submit your questions on-line at any time by entering them into the Q&A panel on the right-hand side of the WebEx desktop
  – On-line questions will be addressed first
• At scheduled intervals during this education session, the audience will be invited to submit questions through the telephone
  – Ask your question by phone at the designated time by pressing * followed by the number one(1) on your keypad
Session Topics

- Welcome and Introductions
- ACA Section 1104: Mandated Operating Rules
- Federally Mandated Eligibility and Claim Status Infrastructure Operating Rule Requirements
  - Discussion Session #1
    - Companion Guide
    - System Availability
    - Real-time Processing Key Rule Requirements
  - Discussion Session #2
    - Connectivity
    - Security
  - Discussion Session #3
    - Trading Partner Collaboration and Testing
- Wrap-Up
ACA Section 1104: Mandated Eligibility and Claim Status Operating Rules

Timeline and Compliance
ACA Mandated Operating Rules Compliance Dates: Required for all HIPAA Covered Entities

Operating rules encourage an interoperable network and, thereby, are vendor agnostic

- Implement by January 1, 2013
  - Eligibility for health plan
  - Claims status transactions

- Implement by January 1, 2014
  - Electronic funds transfer (EFT) transactions
  - Health care payment and remittance advice (ERA) transactions

- Implement by January 1, 2016
  - Health claims or equivalent encounter information
  - Enrollment and disenrollment in a health plan
  - Health plan premium payments
  - Referral certification and authorization
  - Health claims attachments
**Three dates** are critical for industry implementation of the first set of ACA mandated Operating Rules.

*There are two types of penalties* related to compliance.

<table>
<thead>
<tr>
<th>Key Area</th>
<th>HIPAA Mandated Implementation</th>
<th>ACA-required Health Plan Certification</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Dates</strong></td>
<td><strong>First Date</strong>&lt;br&gt;January 1, 2013&lt;br&gt;Compliance Date</td>
<td><strong>Second Date</strong>&lt;br&gt;December 31, 2013&lt;br&gt;Health Plan Certification Date</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td><strong>Who:</strong> All HIPAA covered entities&lt;br&gt;<strong>Action:</strong> Implement CAQH CORE Eligibility &amp; Claim Status Operating Rules</td>
<td><strong>Who:</strong> Health plans&lt;br&gt;<strong>Action:</strong> File statement with HHS certifying that data and information systems are in compliance with the standards and operating rules&lt;sup&gt;2&lt;/sup&gt;</td>
</tr>
<tr>
<td><strong>Applicable Penalties</strong></td>
<td><strong>Amount:</strong> Due to HITECH, penalties for HIPAA non-compliance have increased, now up to $1.5 million per entity per year</td>
<td><strong>Amount:</strong> Fee amount equals $1 per covered life&lt;sup&gt;3&lt;/sup&gt; until certification is complete; penalties for failure to comply cannot exceed on an annual basis an amount equal to $20 per covered life or $40 per covered life for deliberate misrepresentation</td>
</tr>
</tbody>
</table>

<sup>1</sup> CMS OESS is the authority on the HIPAA and ACA Administrative Simplification provisions and requirements for compliance and enforcement. The CMS website provides information on the ACA [compliance, certification, and penalties](https://www.hhs.gov/ocr/privacy/hipaa/hitech/index.html) and [enforcement process](https://www.cms.gov/Regulations-and-Guidance/Legislation/Operational-Rules).  
<sup>2</sup> According to CMS, regulation detailing the health plan certification process is under development, and they will release details surrounding this process later this year; CAQH CORE will continue to offer its voluntary CORE Certification program and will share lessons learned with CMS as the Federal process is developed.  
<sup>3</sup> Covered life for which the plan’s data systems are not in compliance; shall be imposed for each day the plan is not in compliance.
## Mandated Eligibility & Claim Status Operating Rules

**Compliance date January 1, 2013**

### Type of Rule

<table>
<thead>
<tr>
<th>Addresses</th>
<th>CAQH CORE Eligibility &amp; Claim Status Operating Rules</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data Content: Eligibility</strong></td>
<td>Need to drive further industry value in transaction processing</td>
</tr>
<tr>
<td><strong>Infrastructure: Eligibility and Claim Status</strong></td>
<td>Industry needs for common/accessible documentation</td>
</tr>
<tr>
<td></td>
<td>Industry-wide goals for architecture/performance/connectivity</td>
</tr>
</tbody>
</table>

### Voluntary Eligibility & Claim Status Operating Rule

“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.”

**HHS Interim Final Rule**

*Please Note: In the Final Rule for Administrative Simplification: Adoption of Operating Rules for Eligibility for a Health Plan and Health Care Claim Status Transaction, CORE 150 and CORE 151 are not included for adoption. HHS is not requiring compliance with any operating rules related to acknowledgement, the Interim Final Rule.*

---

© 2012 CORE. All rights reserved.
**Federally Mandated CAQH CORE Connectivity Rules: Requirements Scope for HIPAA Covered Entities**

Mandated healthcare operating rules build upon a range of standards – healthcare-specific (e.g., ASC X12) and industry-neutral (e.g., OASIS, W3C, ACH CCD+).

<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><strong>Infrastructure</strong></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><strong>Data Content</strong></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.*
Polling Question

Operating Rule Implementation Status

Which answer best describes the status of your organization’s progress toward implementing the mandated January 1, 2013 operating rules?

– Just started/early phases
– Fully underway/over the hump
– Nearing completion/Done
– Not applicable
Ground Rules and Focus of This Interactive Discussion

• **Federally Mandated CAQH CORE Infrastructure Operating Rules**
  - Companion Guides
  - Connectivity and Security
  - Response Time
  - System Availability

• **CAQH CORE Data Content Operating Rule questions can be submitted to CAQH@CORE.org**

*Acknowledgements standards or the operating rules for those standards are not Federally mandated by HIPAA; CORE operating rules have always included and supported the use of acknowledgements.*
CAQH CORE Eligibility & Claim Status

Federally Mandated Infrastructure Operating Rules
CAQH CORE Eligibility & Claim Status: Federally Mandated Infrastructure Operating Rules

Mandated infrastructure requirements apply to both ASC X12 270/271 eligibility and ASC X12 276/277 claim status transactions

• **Companion Guide**
  – 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

• **Response Time**
  – 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](#)

• **Connectivity Rules**
  – Clients and servers must follow requirements in the CAQH CORE Connectivity Rules: [CAQH CORE Rules 270 and 153](#)

**NOTE:** Many of the Federally mandated CAQH CORE Infrastructure Rules also apply to the ASC X12 v5010 835 per [CMS-0028-IFC](#).
The CAQH CORE Companion Guide Rule and Claim Status Rule require that Companion Guides covering v5010 270/271 and v5010 276/277 transactions follow the format and flow of the CORE v5010 Master Companion Guide Template.

The Companion Guide Template* organizes information into distinct sections:

- General Information
- Connectivity with the payer
- Transaction-Specific Information
- Key contact information
- Testing with the payer
- Control segment details
- Payer specific business rules
- Allows health plans (information sources) to tailor the document to meet their particular needs while still maintaining a standard template/common structure

For more detail, see CORE Rules 152 and 250

The CAQH CORE System Availability Rule and the Claim Status Rule establish guidelines for system availability and provider support for health plan eligibility and claim status transactions including:

- Minimum of **86 percent system availability** (per calendar week)
- Publish regularly scheduled downtime
- Provide one week advance notice on non-routine downtime
- Provide information within one hour of emergency downtime

*For more detail, see CORE Rules 157 and 250*
FAQs: Infrastructure Operating Rules

Response Time Requirements

• When processing in real time, maximum response time for receipt of a v5010 X12 271 or X12 276 by the provider in response to a v5010 X12 270 or X12 276 must be 20 seconds

• To conform to response time requirement, 90 percent of all transactions, as measured within a calendar month, must be returned within the 20-second maximum response time

NOTE: The rules hold the health plan and its contracted business associates responsible for the conduct of the transaction that is applicable to them.

CAQH CORE Rules 156 & 250

When Do the 20-Seconds Begin and End?

• The 20-second requirement is the duration for the entire round trip of the transaction
  – The 20 seconds begin when the v5010 X12 270 Inquiry or X12 276 Request is first submitted by the provider, and end when the X12 271 or X12 277 Response is received by the provider
  – All ensuing hops between the provider and the health plan are included in these 20 seconds

• ACA Administrative Simplification provisions require all HIPAA covered entities (i.e., health plans, providers, clearinghouses, etc.) to comply with the Federally mandated CAQH CORE Eligibility & Claim Status Operating Rules
  – Each HIPAA covered entity within the transaction flow is bound by the CAQH CORE requirements for meeting the 20-second round trip of the transaction

• CAQH CORE recommends a maximum of 4 seconds per hop to meet the 20-second round trip requirement
CAQH CORE Real Time Processing: Potential Real Time Transaction Paths

End-to-End: 20-Second Round Trip
(CAQH CORE recommends no more than 4 seconds per hop)

Path #1: Direct Connection: A+B = 20 seconds or less

Path #2: Single Clearinghouse: A+B+C+D = 20 seconds or less

Path #3: Dual Clearinghouse: A+B+C+D+E+F = 20 seconds or less

At starred receipt and transmit points each entity must capture, log, audit, match, & report date, time, and control numbers from its own internal systems and corresponding data received from its trading partners.
Q&A

Companion Guide
Batch & Real-Time Response
System Availability

Please submit your question:
• By Phone: Press * followed by the number one (1) on your keypad
• Via the Web: Enter your question into the Q&A pane in the lower right hand corner of your screen
Entities must support HTTP/S 1.1 over the public Internet as a transport method for both batch and real-time eligibility inquiry and response transaction, and claim status; they must follow:

- Real-time and/or batch request submission and response pickup guidelines
- Security and authentication requirements
- Response message options and error notification
- Response time, time out parameters and re-transmission guidelines
- Prescriptive submitter authentication, envelope specifications, etc.
- Payload-agnostic, can use to send any type of data

For more detail, see CORE Rules 153, 250 and 270

Phase I & II CAQH CORE Connectivity Rules constitute a “Safe Harbor” rule which provides for a uniform method of exchanging administrative transaction data between health plan and provider –but other methods may be used. The rules:

- Apply to information sources performing the role of an HTTP/S server and information receivers performing the role of an HTTP/S client
- Apply to real-time transactions (and batch, if offered; batch NOT required)
- Do not require trading partners to remove existing connections that do not match the rule
- Include prescriptive submitter authentication, envelope specifications, etc., (SOAP and WSDL, Name/Password or X.509 Certificate)

For more detail, see CORE Rules 153, 250 and 270

*Specifically designed to align with key Federal efforts, e.g., NwHIN.*
Federally Mandated CAQH CORE Connectivity Rules: High Level Rule Requirements

<table>
<thead>
<tr>
<th>CAQH CORE CONNECTIVITY</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>RULE AREA</strong></td>
</tr>
<tr>
<td>Network</td>
</tr>
<tr>
<td>Transport</td>
</tr>
<tr>
<td>Transport Security</td>
</tr>
<tr>
<td>Submitter (Originating System or Client) Authentication</td>
</tr>
<tr>
<td>X 509 Certificate <em>(subject to conformance requirements)</em></td>
</tr>
<tr>
<td>Envelope and Attachment Standards</td>
</tr>
<tr>
<td>Envelope Metadata</td>
</tr>
<tr>
<td>New Payload Types for HIPAA and non-HIPAA Payloads</td>
</tr>
<tr>
<td>Message Interactions/ Routing</td>
</tr>
<tr>
<td>Real time</td>
</tr>
<tr>
<td>Acknowledgements, Errors</td>
</tr>
<tr>
<td>Basic Conformance Requirements</td>
</tr>
<tr>
<td>Response Time</td>
</tr>
<tr>
<td>System Availability</td>
</tr>
<tr>
<td>Companion Implementation Guide</td>
</tr>
</tbody>
</table>
Federally Mandated CAQH CORE Connectivity Rules: Message Structure

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

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

= 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

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"
xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"

<soapenv:Header>
<wsse:UsernameToken xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
<wsu:Id="UsernameToken-21621663">bob</wsu:Id>
<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>
</soapenv:Header>

<soapenv:Body>
<ns1:COREEnvelopeRealTimeRequest xmlns:ns1="http://www.caqh.org/SOAP/WSDL/CORERule2.2.0.xsd">

<ProcessingMode>RealTime</ProcessingMode>
<PayloadID>81d4fabe-7dec-11d0-a765-00a0c916bf6</PayloadID>
<TimeStamp>2007-08-30T10:20:34Z</TimeStamp>
<SenderID>HospitalA</SenderID>
<ReceiverID>PayerB</ReceiverID>
<CORERuleVersion>2.2.0</CORERuleVersion>

<Payload><![CDATA[ISA*00* "00" *ZZ*NEHEN780 *ZZ*NEHEN003 ...IEA1*1*000000031]]></Payload>
</ns1:COREEnvelopeRealTimeRequest>
</soapenv:Body>
</soapenv:Envelope>
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 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)
• 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

- 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 clearinghousesswitches) 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:

<table>
<thead>
<tr>
<th>Health Plan</th>
<th>Clearinghouse/Switch</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Conformance Requirements</td>
<td></td>
</tr>
<tr>
<td>then you must implement both of these envelope standards</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Health Plan</th>
<th>Clearinghouse/Switch</th>
</tr>
</thead>
<tbody>
<tr>
<td>Healthcare Provider</td>
<td></td>
</tr>
<tr>
<td>Client Conformance Requirements</td>
<td></td>
</tr>
<tr>
<td>then you must implement one of these envelope standards</td>
<td></td>
</tr>
</tbody>
</table>

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>Server Conformance Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Health Plan</td>
</tr>
<tr>
<td>then implement one of these authentication standards</td>
</tr>
<tr>
<td>Username/Password</td>
</tr>
<tr>
<td>X.509 Certificate over SSL</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Client Conformance Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clearinghouse/Switch</td>
</tr>
<tr>
<td>Healthcare Provider</td>
</tr>
<tr>
<td>then you must implement both of these authentication standards</td>
</tr>
<tr>
<td>Username/Password</td>
</tr>
<tr>
<td>X.509 Certificate over SSL</td>
</tr>
</tbody>
</table>
Please submit your question:
- **By Phone**: Press * followed by the number one (1) on your keypad
- **Via the Web**: Enter your question into the Q&A pane in the lower right hand corner of your screen
Providers, health plans and clearinghouses work together in a variety of ways to exchange transaction data.

The scope of an entity’s mandated operating rules implementation project will depend upon the electronic data flows between trading partners; understand your agreements.

Vendors play a crucial role in enabling provider clients to realize the benefits of industry adoption of CAQH CORE Operating Rules; engage them.
Testing and Certification:
Trading Partner Listing and Voluntary CORE Certification

- Testing with your trading partners is a critical aspect to making your operating rules implementation a success
  - HIPAA covered entities can quickly communicate their organization’s readiness* to testing their conformance with trading partners by adding their company information to the [CORE Partner Testing](#) page of the CAQH website
  - *If you are ready to test with trading partners, [take 5 minutes and add your organization to the CAQH CORE list!](#)*

- Since its inception, CAQH CORE has offered a voluntary CORE Certification to health plans, vendors, clearinghouses, and providers
  - Learn more about voluntary CORE Certification [here](#)
  - Voluntary CORE Certification provides verification that your IT systems or product operates in accordance with the federally mandated operating rules

* Includes other key IT system/service vendors that support them, such as Practice Management Systems
Q&A

Voluntary CORE Certification & Trading Partner Testing

Please submit your question:
• By Phone: Press * followed by the number one (1) on your keypad
• Via the Web: Enter your question into the Q&A pane in the lower right hand corner of your screen
Upcoming *Free* CAQH CORE Education Events

- CAQH CORE Town Hall Call, December 11, 2012
- *CAQH CORE Open Mic Session with CMS’ Office of E-Health Standards and Services (OESS)*, December 13, 3:30pm-5pm ET
- CAQH and NeHC Joint Session, *Is Your Organization Ready to Meet the Compliance Deadline?*, Tuesday, December 18, 3:00pm - 4:30pm ET
Thank You for Joining Us


Mandated Eligibility & Claim Status Operating Rules

CAQH CORE Eligibility & Claim Status Operating Rules were initially developed in two phases; for ease of use the rules are presented here by transaction addressed and rule type rather than by phase.

• Rules Addressing the **ASC X12 270/271 Eligibility & Benefits Transactions**
  
  – Data Content Related Rules
    • CAQH CORE 154 & 260: Eligibility & Benefits Data Content Rules
    • CAQH CORE 258: Normalizing Patient Last Name Rule for Eligibility
    • CAQH CORE 259: AAA Error Code Rule for Eligibility
  
  – Infrastructure Related Rules
    • CAQH CORE 150: Batch Acknowledgements Rule for Eligibility (999)*
    • CAQH CORE 151: Real Time Acknowledgements Rule for Eligibility (999)*
    • CAQH CORE 152: Companion Guide Rule
    • CAQH CORE 155: Batch Response Time Rule for Eligibility
    • CAQH CORE 156: Real Time Response Rule for Eligibility
    • CAQH CORE 157: System Availability Rule
    • CAQH CORE 153 & CAQH CORE 270: Connectivity Rules

• Rules Addressing the **ASC X12 276/277 Claim Status Transactions**
  
  • CAQH CORE 250: 276/277 Claim Status Infrastructure Rule*

*NOTE: In the Final Rule for Administrative Simplification: Adoption of Operating Rules for Eligibility for a Health Plan and Health Care Claim Status Transaction, 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.”

© 2012 CORE. All rights reserved.
Examples: CAQH CORE Implementation Tools

- **Trading Partner Readiness Site**: Discover which organizations are ready to test their implementation of operating rules with trading partners.
- **FAQs**: CAQH CORE has a list of FAQs to address typical questions regarding the operating rules; updated FAQs being loaded to website as appropriate given mandates.
- **Request Process**: Contact technical experts as needed at CORE@caqh.org.
- **Voluntary CORE Certification**: Phase I & Phase II CORE Certification Master Test Suites provide guidance on the stakeholder types to which the rules apply and working with trading partners; enable conformance testing for implementers.