CAQH CORE Connectivity Rules
Comparison of Rule Requirements Between Current Mandated Versions and Proposed Versions for NCVHS Adoption - November 2022

CAQH CORE Connectivity establishes key connectivity, security and authentication requirements including acknowledgements, error handling, and the CAQH CORE Connectivity "Safe Harbor" creating a national connectivity mechanism that trading partners can be assured will be supported when healthcare information is exchanged. As the healthcare industry continues to progress toward achieving alignment and interoperability across systems and technologies, updating common methods of connectivity and enhancing security is necessary to ensure requirements continue to meet industry need.

▪ The table below compares requirements in the federally mandated Phase I CORE 153: Eligibility and Benefits Connectivity Rule and Phase II CAQH CORE 270: Connectivity Rule to updates made in CAQH CORE Connectivity Rule vC4.0.0.

#	Connectivity Area	Current Mandated CAQH CORE Connectivity Rules ▪ Phase I CORE 153: Eligibility and Benefits Connectivity Rule ▪ Phase II CAQH CORE 270: Connectivity Rule	Proposed CAQH CORE Connectivity Rule for NCVHS Adoption ▪ CAQH CORE Connectivity Rule vC4.0.0
1.	Scope	These rules applies when trading partners exchange any of the X12 transactions addressed by the Eligibility & Benefits, Claim Status, and Payment & Remittance Operating Rules.	The rule applies when trading partners exchange any of the X12 transactions addressed by all published Operating Rules. The rule also supports exchange of non-X12 transactions including (HL7 C-CDA, FHIR Resources, .pdf, etc.).
2.	Standards	**Network**: Public Internet **Transport Protocol**: HTTP/S **Transport Security**: SSL 3.0/TLS 1.0 or higher **Authentication**: Username + Password / X.509 Certificates	**Network**: Public Internet **Transport Protocol**: HTTP/S **Transport Security**: TLS 1.2 or higher **Authentication**: X.509 Certificates **Authorization:** OAuth 2.0
3.	Security	**Authentication:** Servers must implement and enforce one of the two authentication standards. Clients must implement support for both authentication standards.	**Authentication:** Servers and clients must implement the authentication standard. **Authorization:** Servers must implement the authorization standard for SOAP and REST. Clients must implement the authorization standard for REST and optionally implement for SOAP.
4.	**Message Protocol**	SOAP + WSDL; XML HTTP MIME Multipart	SOAP + WSDL; XML REST API; JSON
5.	APIs	**N/A**	The rule requires the use of normative versioning and standard naming conventions for REST API endpoints to streamline uniform REST implementations.
6.	Metadata	**SOAP:** Metadata defined (Field names, values) (e.g., Payload Type, Processing Mode, Sender ID, Receiver ID).	**SOAP:** Metadata defined (Field names, values) (e.g., Payload Type, Processing Mode, Sender ID, Receiver ID) SHA-1 for Checksum FIPS 140-2 compliant implementations can use SHA-2 for checksum. **REST:** HTTP metadata defined for REST request and responses.
7.	**Message Interactions**	Real-time Batch (Optional if used)	Batch and Real-Time processing requirements defined per transaction. Generic push and pull interactions.
8.	**Error Handling**	Specifies error handling processes and messaging requirements via error codes.	Errors Codes updated.

CAQH CORE Connectivity Rules

Comparison of Rule Requirements Between Current Mandated Versions and Proposed Versions for NCVHS Adoption - November 2022

9.	Safe Harbor	Servers must implement the capability to support SOAP and MIME rule requirements. Clients must implement capability to support SOAP or MIME requirements.	Servers must implement the capability to support SOAP and REST rule requirements. Clients must implement capability to support SOAP or REST requirements.