Contents

For CSWG Discussion Only

1. Overview

1.1 Background

The CAQH CORE Connectivity & Security Work Group (CSWG) launched in February 2020 to evaluate opportunities to strengthen CAQH CORE Connectivity Rules and move the industry towards a common set of Safe Harbor connectivity methods that address existing and emerging connectivity standards and security protocols to support the intersection of administrative and clinical data exchange.

Following its Wednesday 02/26/20 call, the CSWG received Feedback Form #1 and were tasked with providing feedback on the opportunity areas and potential updates to CAQH CORE Connectivity Rule requirements and submitting comments for consideration on the Work Group's next call on Wednesday 04/01/20. The information received provided further insight into the impact of potential updates to connectivity rule requirements under consideration by the Work Group.

1.2 Format of Feedback Form

CSWG Feedback Form #1 consisted of six sections, listed below in the order they appeared:

- **Opportunity Area #1**: Potential Updates to CAQH CORE Connectivity Safe Harbor Requirements
- **Opportunity Area #2**: Single, Uniform CAQH CORE Connectivity Rule
- **Opportunity Area #3**: Potential Updates to CAQH CORE Connectivity Transport Security Requirements
- **Opportunity Area #4**: Potential Updates to CAQH CORE Connectivity Submitter Authentication Requirements
- **Opportunity Area #5**: Potential Updates to CAQH CORE Connectivity Message Interactions Requirements
- **Opportunity Area #6**: Potential Updates to CAQH CORE Connectivity API/Web Services Requirements

In each section, respondents were asked to select "Support" or "Do Not Support" to indicate whether their organization supports pursuing each opportunity area listed as part of the update to the CAQH CORE Connectivity Rule. Follow up questions asked respondents for additional feedback pertaining to versioning, specific implementation of the opportunity area, their organization's current use of emerging standards, etc. Respondents were also able to provide clarifying comments relating to their responses.

For CSWG Discussion Only

2. Summary of Feedback Form Respondents

Responses were received from **17** respondents representing **71%** of Connectivity & Security Work Group participating organizations.

Total Number of Individual Responses	17 (71% of the CSWG)
Number of Provider / Provider Association / Provider-Facing Vendor Responses	3 (18% of respondents)
Number of Health Plan / Health Plan Association / Health-Plan Facing Vendor Responses	7 (41% of respondents)
Number of Dual-Facing Vendor / Clearinghouse Responses	4 (23% of respondents)
Number of Government / 'Other' Responses	3 (18% of respondents)

3. Percent Support for Potential Opportunity Areas

When the feedback form closed on Friday, 03/20/20, all six opportunity areas had least **76% support**, as shown in Tables 1 and 2 below.

Table 1. Percent Support for Opportunity Areas 1 and 3 – 6

#	*CSWG Feedback Form #1: Support for Potential Opportunity Areas 1 and 3 - 6*	Support	Do Not Support	Abstain / Do Not Know #
Opportunity Area 1: Safe Harbor				
1	Establish Safe Harbor requirements that are tiered and specific to a set of use cases.	13 (81%)	3 (19%)	1
Opportunity Area 3: Transport Security				
2	Establish requirements to specify the use of TLS 1.2 or higher for transport security. ***NOTE:*** • *69% of respondents voted to specify TLS 1.2 (or higher)* • *31% of respondents voted to specify TLS 1.3*	16 (94%)	1 (6%)	0

For CSWG Discussion Only

#	*CSWG Feedback Form #1: Support for Potential Opportunity Areas 1 and 3 - 6*	Support	Do Not Support	Abstain / Do Not Know #
Opportunity Area 4: Submitter Authentication				
3	Continue to support X.509 Digital Certificate as a submitter authentication requirement.	14 (87%)	2 (13%)	1
4	Pursue additional analysis to add a potential requirement for OAuth as an authentication method. ***NOTE:*** • *53% of respondents' organizations currently use OAuth 2.0* • *47% of respondents' organizations currently do not use OAuth at all* • *None use OAuth 1.0.*	13 (76%)	4 (24%)	0
Opportunity Area 5: Message Interactions				
5	Update Batch/Async message interaction patterns to support Attachments transactions.	11 (85%)	2 (15%)	4
6	Update Real Time/Sync message interaction patterns to support Attachments transactions.	10 (83%)	2 (17%)	5
Opportunity Area 6: API/Web Services				
7	Pursue additional analysis to add a potential requirement to support REST for X12 based exchanges. ***NOTE:*** • *69% of respondent organizations that conduct electronic transactions currently support REST.* • *25% of respondent organizations that conduct electronic transactions currently do **not** support REST.* • *6% of respondent organizations that conduct electronic transactions did not know if their organization supports REST.*	16 (94%)	1 (6%)	0

For CSWG Discussion Only

#	*CSWG Feedback Form #1: Support for Potential Opportunity Areas 1 and 3 - 6*	Support	Do Not Support	Abstain / Do Not Know #
8	Pursue additional analysis to add a potential requirement to support HL7 FHIR for FHIR based exchanges. ***NOTE:*** • *63% of respondent organizations that conduct electronic transactions currently use FHIR in some capacity.* – 10% of these organizations use FHIR version R3. – 40% of these organization use FHIR version R4. – 50% of these organizations did not know what version of FHIR their organization uses. • *38% of respondent organizations that conduct electronic transactions currently do **not** use FHIR.*	15 (94%)	1 (6%)	1

Table 2. Percent Support for Opportunity Area 2

Question #	CSWG Feedback Form #1: Support for Opportunity Area 2 (Single Uniform CAQH CORE Connectivity Rule) Format Options	Option 1: Mandated vs. Voluntary	Option 2: By Transaction	Abstain / Don't Know #
Opportunity Area 2: Single, Uniform CAQH CORE Connectivity Rule				
2	Approach to format and organize a Single, Uniform CAQH CORE Connectivity Rule.	7 (47%)	8 (53%)	2

For CSWG Discussion Only

4. Summary of CSWG Feedback Form Comments Received

Respondents were given the opportunity to provide comments on each of the questions asked on the feedback form. Three categories of comments were received:

1. **Points of Clarification** – Pertain to areas where more explanation for the Work Group is required*; may* require adjustments to the potential CAQH CORE Connectivity Rule Update, which do not change rule requirements.
2. **Substantive Comments** – May impact rule requirements; some comments require Work Group discussion on suggested adjustments to the potential opportunity areas and requirements.
3. **Non-substantive Comments** – Pertain to typographical/grammatical errors, wordsmithing, clarifying language, addition of references; do not impact rule requirements. **NOTE:** Non-substantive comments do not require Work Group discussion, CAQH CORE staff will make these adjustments to the requirements, as necessary. We will not be reviewing these comments on today's call, but they are available here for offline review.

The tables below summarize comments submitted by the CSWG on the Feedback Form. For the substantive comments, the table includes CAQH CORE Co-Chair and staff recommendations, but discussion among the Work Group on these comments is encouraged.

For CSWG Discussion Only

5. Comments Received on CSWG Feedback Form #1

5.1 Comments Received on Opportunity Area #1: Safe Harbor

Table 1 below summarizes comments received from CSWG feedback form respondents pertaining to Opportunity Area #1: Safe Harbor, along with CAQH CORE CSWG Co-chair and staff responses.

Table 1. Comments Received on Opportunity Area #1: Safe Harbor

#	Question	Summary of Comments	CAQH CORE Co-Chair & Staff Response
Points of Clarification			
1	Tiered Safe Harbor Approach	One entity asked for clarification as to whether the Connectivity Update is recommending the removal of username/password as an authentication method.	Developed and approved by CAQH CORE Participating Organizations in 2016, the existing CAQH CORE Phase IV Connectivity Rule removed username/password as a required authentication method and converged to the use of X.509 Digital Certificate as the single authentication standard for the conduct of a subset of X12 standards. The Phase II CORE Connectivity Rule addresses requirements for a different subset of X12 standards. The aim of the CAQH CORE Connectivity Rule Update is to create a single, uniform CAQH CORE Connectivity Rule that includes a safe harbor requirement with base standards that are used across transactions in order to promote interoperability through a structured, yet flexible framework. Organizations may choose to continue using username/password; however, this would not be in conformance with the most current safe harbor requirements and therefore are outside the scope of a CAQH CORE Connectivity Rule.
2	Tiered Safe Harbor Approach	Two entities recommended adjustments to the CAQH CORE Connectivity Rule Update tiered safe harbor approach. • One commented that the requirements need to be stronger (e.g., the rule should require the use of two factor authentication, not the use of one or the other).	Given at least 76% of Work Group respondents voted to pursue the development of OAuth as an additional authentication factor and REST and FHIR APIs as additional web services for the exchange of electronic transactions, CAQH CORE Co-chairs and staff will continue to pursue research and analysis of these methods for inclusion in the CAQH CORE Connectivity Rule Update. CSWG participating organizations will have the opportunity on future feedback forms and straw polls to give feedback as to whether these additional methods should be *in addition to* the base requirements or another

For CSWG Discussion Only

#	Question	Summary of Comments	CAQH CORE Co-Chair & Staff Response
		• The other recommended that when the rule allows for more than one method (e.g. Digital Certificate and/or OAuth; SOAP and/or REST), a provider may support **either** option while health plans and vendors/clearinghouses should be required to support **both** options.	option that can be used *instead of* the base and how a client and server will implement those requirements . Additionally, like prior CAQH CORE Connectivity Rules, the requirements established in the CAQH CORE Connectivity Rule Update are a floor and not a ceiling in terms of what organizations can implement.
Substantive Comments			
3	Tiered Safe Harbor Approach	Two entities commented that there should be one set of connectivity and security requirements that support all healthcare transactions and they should be payload agnostic.	**For CAQH CORE CSWG Discussion.** The aim of the CAQH CORE Connectivity Rule Update is to create one single, uniform connectivity rule with base requirements that could apply to all electronic healthcare transactions (e.g. SOAP). Tiered requirements would allow organizations to implement existing and new requirements specific to a set of use cases, as needed within their organization (e.g. REST, FHIR, etc.). Given 81% of the Work Group supports the tiered approach to the safe harbor opportunity area, CAQH CORE Co-chairs and staff recommend moving forward with the tiered approach as requirements are developed.
Non-Substantive Comments			
4	Tiered Safe Harbor Approach	Two entities explained their support for the tiered safe harbor approach. • One stated that the approach aligns with changes made for Medicare Administrative Contractors (MACs) and Shared System Maintainers (SSMs). • Another noted that industry standards are needed as we move to the work of FHIR over REST and use OAuth and OpenID Connect.	
5	Tiered Safe Harbor Approach	One entity noted that they use a number of different transactions and would like to see a truly payload agnostic standard.	
6	Tiered Safe Harbor Approach	One entity commented that they have security and access requirements outlined by their security division that do not always conform or follow CORE Connectivity requirements. They further explained that their organization does not always implement multiple security and connectivity access options.	

For CSWG Discussion Only

5.2 Comments Received on Opportunity Area #2: Single, Uniform CAQH CORE Connectivity Rule

Table 2 below summarizes comments received from CSWG feedback form respondents pertaining to Opportunity Area #2: Single, Uniform CAQH CORE Connectivity Rule, along with CAQH CORE CSWG Co-chair and staff responses.

Table 2. Comments Received on Opportunity Area #2: Single, Uniform CAQH CORE Connectivity Rule

#	Question	Summary of Comments	CAQH CORE Co-chair & Staff Response
		Points of Clarification	
1	Format of Uniform Rule (*Organized by Mandate Status vs. by Transaction*)	One entity commented that CAQH CORE does not have the authority to establish connectivity requirements for attachments because there is currently not a mandated attachments standard.	CAQH CORE is responsible for engaging the healthcare industry in developing consistent business processes for patients, providers and health plans to streamline the business of healthcare. The CAQH CORE process centers on an integrated model consisting of rule development, education, testing and certification, and measuring/tracking. Since 2012, CAQH CORE has maintained a focus on attachments, collaborating with over 300 healthcare organizations to provide education and gather insights on industry opportunities via operating rule development input, national webinars and surveys in anticipation of an attachments NPRM and its designation as the HHS Operating Rule author. CAQH CORE plans to honor its commitment by incorporating attachments into the CAQH CORE Connectivity Rule Update, in conjunction with the launch the CAQH CORE Attachments Subgroup that will develop operating rules to improve the automation of the exchange of attachments/additional medical documentation with an initial focus on prior authorization use case to move the needle of industry adoption of electronic attachments.
2	Format of Uniform Rule (*Organized by Mandate Status vs. by Transaction*)	One entity clarified that they do not support either option. They suggested that the industry develop one overarching connectivity rule for all transactions. They also commented that CAQH CORE should recommend the connectivity update to be federally mandated.	The aim of the CAQH CORE Connectivity Rule Update is to create a single, uniform CAQH CORE Connectivity Rule that includes a safe harbor requirement with base standards that are used across transactions in order to promote interoperability through a structured, yet flexible framework. The format options presented on the feedback form (Option 1 – Organized by Mandate Status and Option 2 – Organized by Transaction) only reflect how the requirements would be organized and structured within the single connectivity rule; each transaction would have the same base requirements. Finally, the CAQH CORE Board plans to propose the revised Connectivity Operating Rules package to the National Committee on Vital and Health Statistics (NCVHS) for recommendation to the HHS Secretary for national adoption under HIPAA.

For CSWG discussion only

#	Question	Summary of Comments	CAQH CORE Co-chair & Staff Response
3	Format of Uniform Rule (*Organized by Mandate Status vs. by Transaction*)	One entity suggested adding system availability to the CAQH CORE Connectivity Rule Update. They specified that given healthcare is a 24/7 business, the system availability requirement under the updated CAQH CORE Connectivity Rule should be 95% system availability and should apply to all mandated electronic transactions and use cases.	The CAQH CORE Connectivity Rule Update only addresses connectivity and security; therefore, potential updates to system availability requirements are outside the scope of this CAQH CORE Connectivity Rule Update. However, rather than placing the potential requirement update out of scope entirely for rule development, CAQH CORE staff will forward the proposed update to system availability requirements to the appropriate subgroup/work group for consideration within a future Infrastructure Rule Update.

For CSWG Discussion Only

Substantive Comments			
4	Format of Uniform Rule (*Organized by Mandate Status vs. by Transaction*)	Five entities expanded on their reason for supporting either Format Option 1 (*Organized by Mandate Status*) or Format Option 2 (*Organized by Transaction):* • One entity explained their support for Option 1 (*Organized by Mandate Status*) stating that to provide clarity and promote interoperability, mandatory rules should be kept separate from voluntary rules for entities not seeking CORE Certification. They further explained that this is especially important when including standards not adopted through rule making outside an operating rule. • Four entities explained their reason to support Option 2 (*Organized by Transaction*) stating that that the industry needs to adopt a common methodology across all transactions to be effective and splitting it by voluntary vs. mandated creates unnecessary noise.	**For CAQH CORE CSWG Discussion.** To create a single, uniform CAQH CORE Connectivity Rule, CAQH CORE Co-chairs and Staff recommend updating *Section 3.3. When the Rule Applies* of the CAQH CORE Connectivity Rule to include all X12 transactions addressed by CAQH CORE Operating Rules, both mandated and voluntary. Similar to the approach taken in the existing CAQH CORE Phase IV Connectivity Rule, Section 3.3., will also include a reference to the CAQH CORE Phase II Connectivity Rule clarifying that while the requirements in the updated CAQH CORE Connectivity Rule support all listed X12 transactions, HIPAA-covered entities must continue to support the requirements established in the ACA-mandated CAQH CORE Phase II Connectivity Rule. While the CAQH CORE Connectivity Rules will specify requirements for all X12 transactions addressed in CAQH CORE Operating Rules, the connectivity and security requirements can be optionally applied to other payload types (e.g. C-CDA, .pdf., .doc, etc.). CAQH CORE Co-chairs and staff will develop a draft Section 3.3 for Work Group feedback on the straw poll following our next call (Call #3) where CSWG participating organizations will have the opportunity to submit feedback on the details of the draft scope section. Finally, the CAQH CORE Board plans to propose the revised Connectivity Operating Rules package to the National Committee on Vital and Health Statistics (NCVHS) for recommendation to the HHS Secretary for national adoption under HIPAA.

For CSWG Discussion Only

5.3 Comments Received on Opportunity Area #3: Transport Security

Table 3 below summarizes comments received from CSWG feedback form respondents pertaining to Opportunity Area #3: Transport Security, along with CAQH CORE CSWG Co-chair and staff responses.

Table 3. Comments Received on Opportunity Area #3: Transport Security

#	Question	Summary of Comments	CAQH CORE Co-chair & Staff Response
Points of Clarification			
1	TLS Version	One entity suggested conducting additional research to determine the potential costs to physicians of implementing the different TLS versions.	CAQH CORE will continue to coordinate with CAQH CORE CSWG participants and other industry stakeholders to understand the feasibility and impacts of the revised CAQH CORE Connectivity requirements. Additionally, CSWG participating organizations will have the opportunity on future feedback forms and straw polls to give feedback on detailed rule requirements that the CSWG chooses to pursue.
Substantive Comments			
2	TLS Version	Three entities explained their support for specifying TLS 1.2 or higher in the rule requirement rather than specifying TLS 1.3: • One stated that the minimum version (TLS 1.2) that offers the level of protection their organization is seeking should be chosen in order to minimize impact on implementing organizations and therefore maximize industry adoption. • One commented that the CAQH CORE rules should support current standards (TLS 1.2) and not set the floor above the current standard. • Another noted that some providers systems are too old to even support TLS 1.2.	**For CAQH CORE CSWG Discussion.** Given 94% of CSWG feedback form respondents supported specifying TLS 1.2 or higher (either TLS 1.2 or higher **or** TLS 1.3) and 69% of respondents supported specifying TLS 1.2 or higher, CAQH CORE Co-chairs and staff recommend moving forward with requirements to support TLS 1.2 or higher to promote adoption and therefore interoperability throughout the industry.
3	TLS Version	One entity suggested that the CAQH CORE Connectivity Rule Update should not specify a version, but instead should specify any TLS standard that is not deprecated by the Internet Engineering Task Force.	**For CAQH CORE CSWG Discussion.** CAQH CORE Co-chairs and staff suggest adding a maintenance requirement to the CAQH CORE Connectivity Rule Update to address the need to regularly update and modify the security transport standard

For CSWG Discussion Only

#	Question	Summary of Comments	CAQH CORE Co-chair & Staff Response
			used in the rule in order to meet changing industry needs as transport security capabilities continue to develop and strengthen. Additionally, specifying a particular version of a standard is necessary for entities building interoperable systems and supports the development of voluntary CORE Certification test scripts, testing engine, etc.
Non-Substantive Comments			
4	TLS Version	One entity explained that they support staying current with the latest best practices for transport security.	

5.4 Comments Received on Opportunity Area #4: Submitter Authentication

Table 4 below summarizes comments received from CSWG feedback form respondents pertaining to Opportunity Area #4: Submitter Authentication, along with CAQH CORE CSWG Co-chair and staff responses.

Table 4. Comments Received on Opportunity Area #4: Submitter Authentication

#	Question	Summary of Comments	CAQH CORE Co-chair & Staff Response
Points of Clarification			
1	Continue to Support X.509 Digital Certificate & Pursue OAuth Requirement(s)	One entity clarified that they support continuing to require X.509 Digital Certificate if it is used in conjunction with another authentication factor (e.g. OAuth, Username/Password, etc.). They also commented that they support pursuing OAuth requirements if required in conjunction with another authentication factor (e.g. X.509 Digital Certificate, Username/Password, etc.).	Given at least 76% of Work Group respondents voted to pursue the development of OAuth as an authentication requirement, CAQH CORE Co-chairs and staff will continue to pursue the research and analysis for the inclusion of this authentication method in the CAQH CORE Connectivity Rule Update. CSWG participating organizations will have the opportunity on future feedback forms and straw polls to give feedback as to whether the base requirement under CAQH CORE Safe Harbor will be X.509 Digital Certificate **and** OAuth or X.509 Digital Certificate **or** OAuth. However, like prior versions of CAQH CORE Connectivity Rules, the requirements established in the CAQH CORE Connectivity Rule Update are a floor and not a ceiling in terms to what organizations can implement.

For CSWG discussion only

#	Question	Summary of Comments	CAQH CORE Co-chair & Staff Response
2	Pursue OAuth Requirement(s)	Two entities commented that they support exploring OAuth as an authentication method for appropriate implementations, depending on use case and transaction.	Given 81% of CSWG respondents supported a tiered approach to the CAQH CORE Connectivity Rule Update, which would specify new connectivity and security requirements based on a set of use cases, the CSWG will pursue the approach described by the commenters.
3	Pursue OAuth Requirement(s)	One entity suggested conducting an impact analysis on the adoption and implementation of OAuth by small medical practices that may not have access to the most sophisticated technology. They also recommended that additional analysis and research should consider the risk of system insecurity associated with incorrect implementation of OAuth and consider measures for mitigating any confusion.	CAQH CORE will continue to coordinate with CAQH CORE CSWG participants and other industry stakeholders to understand the feasibility and impacts of the revised CAQH CORE Connectivity requirements. Additionally, CSWG participating organizations will have the opportunity on future feedback forms and straw polls to give feedback on detailed rule requirements that the CSWG chooses to pursue.
Substantive Comments			
4	Continue to Support X.509 Digital Certificate	One entity expressed concern that if X.509 Digital Certificate is included in the rule, it could be a roadblock to the rule being mandated under HIPAA. They suggested a carve out for X.509 Digital Certificate and that the rule require username/password and/or alternative, stronger authentication methods as the base standard.	**For CAQH CORE CSWG Discussion.** Given 87% of CSWG respondents support continuing to include X.509 Digital Certificate in the CAQH CORE Connectivity Rule Update, CAQH CORE CSWG Co-chairs and staff recommend maintaining the requirement for X.509 Digital Certificate as an authentication method in the updated CAQH CORE Connectivity Rule. Organizations may choose to continue using username/password; however, this would not be in conformance with the most current safe harbor requirements and therefore are outside the scope of a CORE Connectivity Rule. Finally, the CAQH CORE Board plans to propose the revised Connectivity Operating Rules package to the National Committee on Vital and Health Statistics (NCVHS) for recommendation to the HHS Secretary for national adoption under HIPAA.

For CSWG Discussion Only

#	Question	Summary of Comments	CAQH CORE Co-chair & Staff Response
5	Pursue OAuth Requirement(s)	One entity noted that since the ONC Interoperability Rule does not extend the use of FHIR based APIs to transactions between covered entities for purposes of adjudication of transactions for which HIPAA has adopted a standard, OAuth may have the same adoption issues as X.509 Digital Certificate.	**For CAQH CORE CSWG Discussion.** Given 76% of CSWG respondents support pursuing additional research and analysis to include OAuth as a potential requirement in the CAQH CORE Connectivity Rule Update, CAQH CORE CSWG Co-chairs and staff recommend continued research on the potential requirements. CSWG participating organizations will have the opportunity on future feedback forms and straw polls to give feedback on detailed rule requirements. Additionally, the CAQH CORE Board plans to propose the revised Connectivity Operating Rules package to the National Committee on Vital and Health Statistics (NCVHS) for recommendation to the HHS Secretary for national adoption under HIPAA.
Non-Substantive Comments			
6	Continue to Support X.509 Digital Certificate	Two entities commented that they support continuing to require X.509 Digital Certificate as an authentication method. • One entity noted that while X.509 Digital Certificate is the current best practice; the updated connectivity rule needs to allow for future technical evolution. • The other explained that while they support continuing to pursue X.509 Digital Certificate, they have not found that it has high user adoption in the healthcare industry.	
7	Pursue OAuth Requirement(s)	Two entities explained that they support pursuing OAuth requirements in the Connectivity Update. • One clarified that the update to the CAQH CORE Connectivity Rule needs to allow for future technical evolution. • The other stated that OAuth 2.0 and OpenID Connect are currently being explored within their organization for all APIs.	

For CSWG Discussion Only

5.5 Comments Received on Opportunity Area #5: Message Interactions

Table 5 below summarizes comments received from CSWG feedback form respondents pertaining to Opportunity Area #5: Message Interactions, along with CAQH CORE CSWG Co-chair and staff responses.

Table 5. Comments Received on Opportunity Area #5: Message Interactions

#	Question	Summary of Comments	CAQH CORE Co-chair & Staff Response
Points of Clarification			
1	Update Real-Time/Sync Requirements to Support Attachments	One entity clarified that their organization supports real-time receipt of attachments and subsequent acknowledgements but does not support real-time processing of attachments through complete downstream systems.	The aim of Opportunity Area #5 is to update the message interaction patterns currently specified in the CAQH CORE Phase IV Connectivity Rule to support attachments transactions. The updates will include both real time and batch interaction pattern examples. Requirements addressing acknowledgement and any subsequent processing of the attachment transaction will be addressed in the CAQH CORE Attachments Subgroup – PA use case, launching late-April 2020, followed by the claims use case later this year.
2	Update Batch/Async Requirements to Support Attachments **And** Real-Time/Sync Requirements to Support Attachments	Two entities commented that their organization does not support attachments transactions. One of these entities also noted that their organization does not support attachments and potential security of the binary data.	The CAQH CORE Connectivity Rule Update does not require organizations to support the X12 275 transaction or other attachment standards. However, organizations are encouraged to submit feedback as to their support for developing requirements for these and other attachment standards via feedback forms, straw polls and on calls even if their organization does not support an attachment standard today.

For CSWG Discussion Only

Substantive Comments			
3	Update Real Time/Sync Requirements to Support Attachments	Two entities commented that requirements related to the support of attachment standards should not be included in the CAQH CORE Connectivity Update as they may be premature and that system processing requirements for real time processing of an attachment standard payload are not clearly understood by the industry. • One entity noted that since there is no federally mandated electronic standard for attachments, it is difficult to make informed recommendations regarding operating rule requirements. Thus, operating rule requirements for attachments are premature and should not be included in the CORE Connectivity Rule Update. ***NOTE**: This organization's comment applied to both batch and real time message interactions.* • One entity explained that the processing of any attachment standard in a real-time message has a significant impact on the overall processing time and may negatively affect processing times. Therefore, they recommend not updating the real-time requirements to support attachments.	**For CAQH CORE CSWG Discussion.** Given 83% of CSWG respondents supported updating the existing real-time/sync requirements included in CAQH CORE Phase IV Connectivity Rule to support attachments standards, CAQH CORE Co-chairs and staff recommend pursuing these requirements in the CAQH CORE Connectivity Update to move the needle of industry adoption of electronic attachments. CSWG participating organizations will have the opportunity on future feedback forms and straw polls to give feedback on detailed rule requirements and their applicability to industry stakeholders. Requirements addressing processing of an attachment payload may be addressed in the CAQH CORE Attachments Subgroup – PA use case, launching late-April 2020, followed by the claims use case later this year.
Non-Substantive Comments			
4	Update Batch / Async **And** Real Time/Sync Requirements to Support Attachments	One entity explained their organization's support for the requirements stating that their organization recommends a safe harbor rule that supports all transactions and transmission models (batch & real time). ***NOTE**: This comment applied to both batch and real time message interactions.*	

For CSWG Discussion Only

5.6 Comments Received on Opportunity Area #6: API/Web Services

Table 6 below summarizes comments received from CSWG participants pertaining to Opportunity Area #6: API/Web Services, along with CAQH CORE CSWG Co-chair and staff responses.

Table 6. Comments Received on Opportunity Area #6: API/Web Services

#	Question	Summary of Comments	CAQH CORE Co-chair & Staff Response
Points of Clarification			
1	Pursue HL7 FHIR Requirements	One entity commented that they needed more detailed information on the intent of the potential requirement before their organization can vote to support it.	The intent of a potential HL7 FHIR rule requirement is to enable progress in the automation of electronic transactions and support the convergence of clinical and administrative data. All rule requirements will be developed and voted on by the Work Group but would include enabling data sharing between administrative and clinical systems, creating a shared connectivity environment within and across organizations. Further, the rule could require a Safe Harbor for industry that includes the support of HL7 FHIR exchanges with associated authentication methods (e.g., OAuth), with expectations that data is exchanged securely over the public internet, establishing an updated national floor for connectivity. These requirements may be use-case driven to meet specific industry needs. CSWG participating organizations will have the opportunity on future feedback forms and straw polls to give feedback on detailed rule requirements and their applicability to industry stakeholders.
Non-Substantive Comments			
2	Pursue HL7 FHIR Requirements	One entity noted that while they are supportive of the use of APIs in the industry for trading HIPAA standard transactions, they caution that inclusion of APIs as a requirement could disrupt adoption efforts for this rule and suggest that the adoption of operating rules under HIPAA is the best way to achieve administrative simplification and interoperability.	
3	Pursue REST Requirements	One entity noted that their organization started to move towards REST.	

For CSWG Discussion Only

#	Question	Summary of Comments	CAQH CORE Co-chair & Staff Response
4	How REST is Currently used	Seven entities expressed their support for including REST as a CORE Connectivity requirement and described how REST is currently being used within their organizations: • One entity stated that REST is used to call between internal applications. • Another entity commented that their organization would be migrating all connectivity to REST/JSON and sunsetting SOAP/WSDL support in the future. • Another said that their organization uses REST for FHIR based interactions and for other non-FHIR contemporary APIs. They clarified that SOAP/SML is becoming the exception. • Another explained that REST is used to transmit payloads between systems. They also have an API offering that integrators can use to submit eligibility and claims benefit requests. • Another commented that their organization has RESTful APIs for partner integration with revenue cycle features. • Another noted that their organization supports one FHIR transaction (which is RESTful) as well as many REST APIs that are not for data exchange (non-EDI). • Another stated that their organization supports REST services-oriented architecture for business-to-business and application development.	
5	Pursue HL7 FHIR Requirements	Eight entities expressed their support for pursuing HL7 FHIR requirements in the Connectivity Update and explained how their organization is currently using FHIR: • One entity commented that as a payer, supporting FHIR will increase the ability to receive information faster. • Another suggested that the integration of FHIR into the CORE Connectivity Rules may be an appropriate link to supporting attachments. • Another explained that their organizations is exploring how to accept FHIR resources in a data exchange. • Another noted that their organization is currently looking into FHIR. • Another commented that their organization is part of Da Vinci and they support the use of FHIR. • Another said that their organization is undergoing the migration to FHIR for the CMS and ONC rules and will be looking at other opportunities to exchange FHIR based data for a variety of use cases. • Another commented that at their organization FHIR is the preferred methodology where appropriate and where HIPAA X12 is not mandated. • Another noted that their organization supports SMART on FHIR for patients because of the strong nomenclature definitions for data mapping.	

For CSWG Discussion Only

6. Next Steps

- CAQH CORE CSWG Co-Chairs and Staff will:
  - Draft a call summary for today's call for review and approval on our next Work Group call.
  - Draft select scope and requirement sections for review on the Work Group's next call.
- Connectivity & Security Work Group participants will:
  - Attend Connectivity & Security Work Group Call #3 on **Wednesday, 04/29/20 from 2:00 PM – 3:30 PM ET.**
  - Review updated CSWG Activity Schedule included in the appendix of this document.

For CSWG Discussion Only

7. Appendix

Table 1. CAQH CORE Connectivity Rule Update: Opportunity Areas & Initial Recommended Approach

#	Connectivity Area	Opportunity Area	Proposed Approach for Updating the CAQH CORE Connectivity Rule
1	**CAQH CORE Connectivity Rule**	Single CAQH CORE Connectivity Rule	▪ Draft one uniform CAQH CORE Connectivity Rule. ▪ Add in Phase I & II CORE Connectivity requirements. ▪ Organize rule by use cases: – CAQH CORE Connectivity for Eligibility, Claim Status and EFT/ERA. – CAQH CORE Connectivity for Prior Authorization, Claims, Enrollment/Disenrollment, Premium Payment and Attachments.
2	**Network**	Public Internet	▪ Require the transport of data to occur over the public internet as established in the Phase I CAQH CORE Connectivity Rule.
3	**Transport Protocol**	HTTP/S	▪ Require the use of HTTP/S secure transport protocol for data exchange as established in the Phase I CAQH CORE Connectivity Rule.
4	**Transport Security**	SSL	▪ Sunset operating rule requirements that specify the use of SSL. ▪ SSL 2.0 and 3.0 has been deprecated by the Internet Engineering Task Force.
		TLS	▪ Update operating rule requirements that specify the use of TLS. ▪ Update requirements to specify TLS version TLS 1.2 or higher to align with NIST Special Publication (SP) 800-52 Revision 2.
5	**Authentication**	Digital Certificate	▪ Continue supporting Digital Certificate as an authentication requirement.
		OAuth	▪ Update authentication rule requirements to add support for OAuth.
6	**Message Interactions**	Real-Time/Sync	▪ Update Real-Time / Sync message interaction patterns to support Attachment Transactions.
		Batch/Async	▪ Update Batch / Async message interaction patterns to support Attachment Transactions.
7	**API / Web Services**	SOAP	▪ Continue supporting SOAP as a message envelope standard for the exchange of X12 transactions.
		REST	▪ Update rule requirements to add support for REST for the exchange of X12 transactions.
		HL7 FHIR	▪ Update rule requirements to add support for HL7 FHIR for FHIR based exchanges.
8	**Safe Harbor**	Base Requirements	▪ Establish connectivity and security rule requirements to be used across all exchanges.
		Tiered Options	▪ Establish connectivity and security rule requirements that are specific to a set of use cases.

Table 2. Updated CAQH CORE Connectivity & Security Work Group Activity Schedule

Date	Task Group Activity	Topic
Weds 02/26/20 2:00 – 3:30 PM ET	CSWG Call #1	▪ Review CSWG workplan and participant expectations. ▪ Provide summary of CAQH CORE work on Connectivity completed to date including the recent white paper and requirement options that arose in the Attachments Advisory Group. ▪ Orient CSWG to Feedback Form #1.
Fri 02/28/20 – Fri 03/13/20	CSWG Feedback Form #1	▪ Collect information on CSWG support for recommendations to update CAQH CORE Connectivity Rules.
Weds 04/01/20 2:00 – 3:30 PM ET	CSWG Call #2	▪ Review of results of Feedback Form #1.
Weds 04/29/20 2:00 – 3:30 PM ET	CSWG Call #3	▪ Review select draft scope and rule requirement sections. ▪ Orient CSWG to Straw Poll #1.
Fri 05/01/20 – Fri 05/15/20	CSWG Straw Poll #1	▪ Collect level of support from CSWG on support for select draft scope and rule requirement sections for the CAQH CORE Connectivity Update. ▪ Feedback will be used to further develop and refine scope and rule requirements that will be straw polled again after CSWG Call #4.
Weds 05/27/20 2:00 – 3:30 PM ET	CSWG Call #4	▪ Review results from Straw Poll #1. ▪ Orient CSWG to Straw Poll #2.
Fri 05/29/20 – Fri 06/12/20	CSWG Straw Poll #2	▪ Collect level of support from CSWG on Draft CAQH CORE Connectivity Rule Update requirements and updated 'front matter'.
Weds 06/24/20 2:00 – 3:30 PM ET	CSWG Call #5	▪ Review results from Straw Poll #2. ▪ Review Draft Rule prior to CSWG Ballot.
Fri 06/26/20 – Fri 07/17/20	CSWG Ballot	▪ Approve CAQH CORE Connectivity Rule Update.
Weds 07/29/20 2:00 – 3:30 PM ET	*TENTATIVE* CSWG Call #6	▪ Review of substantive comments received on the CSWG Ballot, as needed. ▪ Approve Rule and forward to CORE Final Vote.

For C