Phase IV CAQH CORE Operating Rules Set v4.1.0

February 2020

Table of Contents

Phase IV CAQH CORE 450 Health Care Claim (837) Infrastructure Rule v4.0.0

September 2015

Table of Contents

CAQH Committee on Operating Rules for Information Exchange (CORE)
Phase IV CAQH CORE Operating Rules Set
February 2020

1 Background Summary

Each Phase of CAQH CORE Operating Rules builds on the previous Phases of CAQH CORE Rules to encourage feasible industry progress. Continuing to build on the Phase I, II, and III CAQH CORE Operating Rules, CAQH CORE determined that Phase IV should be extended to include rules around the health care claims and equivalent encounter information transactions to allow the industry to leverage its investment in the Phase I, II, and III CAQH CORE infrastructure rules and apply them to conducting the ASC X12N 005010X222 Health Care Claim (837) Professional, ASC X12N 005010X223 Health Care Claim (837) Institutional, and ASC X12N 005010X224 Health Care Claim (837) Dental transactions and their respective errata (collectively hereafter ASC X12N v5010 837 Claim) including the use of acknowledgements for electronic claims by specifying the use of the following standard electronic acknowledgments when conducting the ASC X12N v5010 837 Claim:

- The ASC X12C 005010X231 Implementation Acknowledgement for Health Care Insurance (999) Technical Report Type 3 (TR3) and associated errata (hereafter ASC X12C v5010 999)
- The ASC X12N 005010X214 Health Care Claim Acknowledgement (277) Technical Report Type 3 (TR3) and associated errata (hereafter ASC X12N v5010 277CA).

Benefits to the industry from applying the CAQH CORE infrastructure rules to health care claims include:

- Less staff time spent on phone calls and websites
- Increased ability to conduct targeted follow-up
- More accurate and efficient processing of claims

The inclusion of this Phase IV CAQH CORE Operating Rule will facilitate the industry's momentum to increase access to the HIPAA-mandated administrative transactions, increase access to the claim acknowledgment transaction, and will encourage all HIPAA-covered entities, business associates, intermediaries, and vendors to build on and extend the infrastructure they have established for CAQH CORE Phases I, II, and III.

1.1 Affordable Care Act Mandates

This CAQH CORE Rule is part of a set of rules that addresses requirements in Section 1104 of the Affordable Care Act (ACA). Section 1104 contains an industry mandate for the use of operating rules to support implementation of the HIPAA standards. Using successful, yet voluntary, national industry efforts as a guide, Section 1104 defines operating rules as "the necessary business rules and guidelines for the electronic exchange of information that are not defined by a standard or its implementation specifications." As such, operating rules build upon existing healthcare transaction standards. The ACA outlines three sets of healthcare industry operating rules to be approved by the Department of Health and Human Services (HHS) and then implemented by the industry.

The third set of ACA-mandated operating rules address the health care claims or equivalent encounter information transaction, enrollment and disenrollment in a health plan, health plan premium payments, claims attachments, and referral certification and authorization.[1] The ACA requires HHS to adopt a set of operating rules for these five transactions by July 2014.[2] In a letter dated 09/12/12 to the Chairperson of the National Committee on Vital and Health Statistics (NCVHS),[3] the Secretary of HHS designated CAQH CORE as the operating rule authoring entity for the remaining five HIPAA-mandated electronic transactions.

[1] The first set of operating rules under ACA Section 1104 applies to eligibility and claim status transactions; these operating rules were effective 01/01/13. The second set of operating rules applies to EFT and ERA; these operating rules were effective 01/01/14.
[2] This date is statutory language and statutory language can be changed only by Congress.
[3] 09/12/12 HHS Letter from the Secretary to the Chairperson of NCVHS.

Section 1104 of the ACA also adds the health claims attachment transaction to the list of electronic healthcare transactions for which the HHS Secretary must adopt a standard under HIPAA. The ACA requires the health claims attachment transaction standard to be adopted by 01/01/14, in a manner ensuring that it is effective by 01/01/16.[4]

NOTE: HHS has not adopted a standard for health claims attachments or indicated what standard(s) it might consider for the transaction, and an effective date for these operating rules is not included in the ACA. Thus, the immediate focus of the Phase IV CAQH CORE Operating Rules will not include attachments.

2 Issue to Be Addressed and Business Requirement Justification

By promoting consistent connectivity methods between providers, health plans, vendors, and clearinghouses, manual processes for claims processing can be reduced and electronic transaction usage increased. Defining acceptable acknowledgement response times, appropriate Batch and Real Time acknowledgements, system availability, and requiring entities that publish a Companion Guide do so in a common standard format to ensure that trading partners are informed of the nuances required for successful transaction processing will allow the industry to more easily adopt the ASC X12N v5010 837 Claim transaction.

In Phase I several CAQH CORE Infrastructure Operating Rules were approved that are designed to bring consistency and to improve the timely flow of the eligibility transactions. These infrastructure rules require:

- Real Time exchange of eligibility transactions within 20 seconds or less
- The consistent use of the ASC X12C v5010 999 for both Real Time and Batch exchanges
- 86% system availability of a HIPAA-covered health plan's eligibility processing system components over a calendar week
- Use of the public internet for connectivity
- Use of a best practices Companion Guide template for format and flow of Companion Guides for entities that issue them

In Phases II and III these CAQH CORE infrastructure rules were applied to the exchange of the HIPAA-mandated ASC X12N 005010X212 Health Care Claim Status Request and Response (276/277) transactions and the HIPAA-mandated ASC X12N 005010X221A1 Health Care Claim Payment/Advice (835) transaction. Phases II and III also included more robust, prescriptive, and comprehensive connectivity requirements.

During the Phase IV CAQH CORE rule development, CAQH CORE used discussion, research, and straw poll results to determine which infrastructure requirements should be applied to the exchange of the ASC X12N v5010 837 Claim transaction. Listed below is an overview of the infrastructure requirements incorporated into this rule in §4.

[4] These dates are statutory language and statutory language can be changed only by Congress.

Phase IV Infrastructure Requirements for the ASC X12N v5010 837 Claim Transaction	
CAQH CORE Infrastructure Requirement Description	**Apply to Phase IV CAQH CORE Infrastructure Rule for the ASC X12N v5010 837 Claim**
Processing Mode*	**Y**
Connectivity	**Y**
System Availability	**Y**
Real Time Processing Mode Response Time	**Y**
Batch Processing Mode Response Time	**Y**
Real Time Acknowledgements	**Y**
Batch Acknowledgements	**Y**
Companion Guide	**Y**
***Note:** Beginning with Phase IV CAQH CORE Infrastructure Rules, processing mode requirements will be explicitly clarified. In previous phases this requirement was not as explicit as needed resulting in questions from implementers. The Phase IV CAQH CORE 470 Connectivity Rule v4.0.0 specifies the processing mode(s) that must be supported for each transaction addressed in Phase IV CAQH CORE Operating Rules.	

This Phase IV CAQH CORE 450 Health Care Claim (837) Infrastructure Rule defines the specific requirements that HIPAA-covered health plans or their agents[5] and HIPAA-covered providers or their agents must satisfy. As with all CAQH CORE Operating Rules, these requirements are intended as a base or minimum set of requirements, and it is expected that many entities will go beyond these requirements as they work towards the goal of administrative interoperability. This Phase IV CAQH CORE 450 Health Care Claim (837) Infrastructure Rule requires that HIPAA-covered health plans or their agents make appropriate use of the claim acknowledgements, support the CAQH CORE connectivity requirements, and use the CAQH CORE v5010 Master Companion Guide Template when publishing their ASC X12N v5010 837 Claim Companion Guide.

By applying these CAQH CORE infrastructure requirements to the conduct of the ASC X12N v5010 837 Claim transaction, this Phase IV CAQH CORE 450 Health Care Claim (837) Infrastructure Rule helps provide claim information electronically and thus reduce the current cost of today's manual transaction processes.

It is understood that applying the CAQH CORE infrastructure requirements to the exchange of the ASC X12N v5010 837 Claim transaction does not address the industry's transaction data content needs but rather establishes an electronic "highway". Subsequent phases of CAQH CORE rule-making may use the industry's experience and lessons learned from implementing this Phase IV CAQH CORE 450 Health Care Claim (837) Infrastructure Rule to develop a CAQH CORE Operating Rule addressing the data content of this transaction.

2.1 Claim Acknowledgements

This Phase IV CAQH CORE 450 Health Care Claim (837) Infrastructure Rule contains specific requirements for claim acknowledgements. Providers have a critical business need to know as quickly as possible whether or not the HIPAA-covered health plan received the claim and then whether the claim was rejected or received into the HIPAA-covered health plan's adjudication system. Often, the claim is rejected early in the information exchange path by intermediaries between the provider and HIPAA-covered health plan. Alternatively, the claim can be received by the HIPAA-covered health plan but not enter the HIPAA-covered health plan's adjudication system. In either case, the provider does not know with certainty that the claim was received by the HIPAA-covered health plan.

These issues represent not just a single problem to be resolved, but a chain of related but different problems that impact both the claim and the ability of the provider to determine the status of the claim, which requires different

[5] One who agrees and is authorized to act on behalf of another, a principal, to legally bind an individual in particular business transactions with third parties pursuant to an agency relationship. Source: West's Encyclopedia of American Law, edition 2. Copyright 2008 The Gale Group, Inc. All rights reserved.

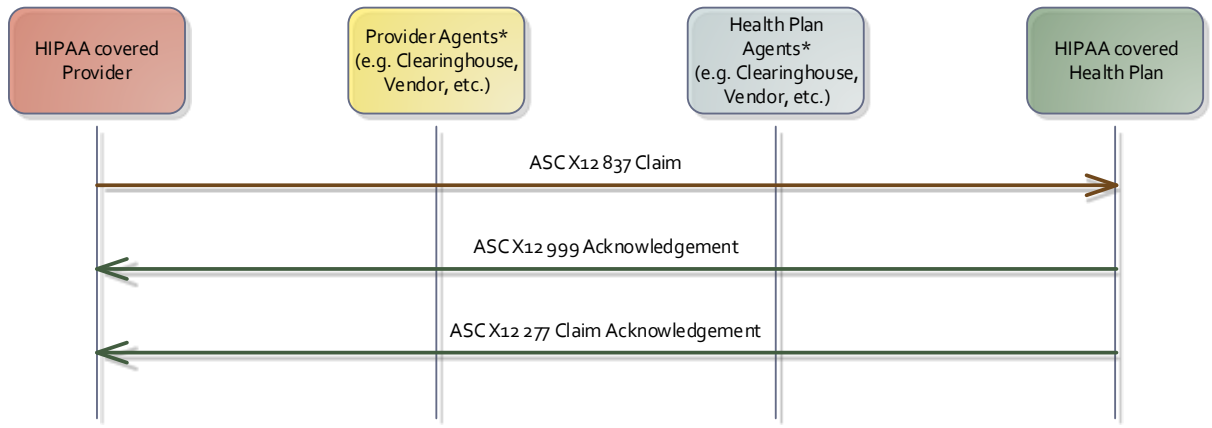
solutions along the chain of information exchanges.[6] The information exchange can vary from a simple provider-direct-to-health plan exchange to a much more complex exchange from the provider through one or multiple clearinghouses or other intermediaries to the health plan. At each point (node) on this information exchange path the information goes through several processes during which a variety of validations and editing are performed. Some of these validation/editing processes may include:

- Claim scrubbing on behalf of the provider
- Receiving a standard interchange and forwarding it to HIPAA-covered health plan or the HIPAA-covered health plan's clearinghouse
- Opening the interchange and applying a HIPAA-covered health plan's business edits on behalf of the HIPAA-covered health plan
- Opening the interchange and reformatting into a proprietary file format for the HIPAA-covered health plan
- Opening a proprietary file and reformatting it into the standard interchange for forwarding to the HIPAA-covered health plan

Figure 1 below is a visual representation of the problem space and information exchanges that are the focus of this rule. Analysis of Figure 1 indicates that the problem space can be generally described as "*Providers need to know whether or not the claim is received and then whether it makes it successfully into the payer's adjudication system."* This problem space can be defined to encompass the point of submission of a claim by a provider to the point that the claim is accepted into a health plan's adjudication system. This problem space includes both the direct submission of a claim to the health plan and the use of one or more intermediaries (e.g., clearinghouses, repricers, etc.) between the provider and the health plan.

[6] Currently, the information exchanges can be either an ASC X12 Interchange of an ASC X12N v5010 837 Claim, an ASC X12 TA1 Interchange Acknowledgment, an ASC X12C v5010 999 Implementation Acknowledgment, an ASC X12N v5010 277 Claim Acknowledgment, or a proprietary report format.

Figure 1: Problem Space and Information Exchanges



- This Sequence Diagram depicts only the direction of the transaction being exchanged and the order (sequence) in which the exchanges take place
- Exchanges may be accomplished in either Real Time or Batch Processing mode
- The elapsed time of the exchange of a transaction between the two HIPAA covered entities and their respective agents is not shown
- This Sequence Diagram does not include any aspect of a Real Time Adjudication process

*Note: Services and other activities performed by an agent are considered to be performed on behalf of the HIPAA covered entity in the role of a Business Associate.

An ASC X12N v5010 837 Claim transaction set undergoes several processing steps before being allowed into the payer's adjudication system, e.g.:

- Verification that the Interchange, Functional Group, and Transactions conform to the ASC X12 standard and implementation specification
- Verification that the claim passes all payer-specific business edits and is allowed to enter into adjudication

Currently, when an ASC X12N v5010 837 Claim transaction set (or a single claim within a transaction set, i.e., unit of work) fails to pass ASC X12 validation, ASC X12 TR3 validation, or payer-specific business edits there is no single industry-wide mechanism to report such rejections to the provider in a standard and consistent format. Lack of a standard report mechanism using standardized data, codes, error messages, etc., hinders the provider's ability to reasonably process myriad reports received and manage their revenue cycle of claim-to-cash effectively and efficiently.

Methods currently employed inconsistently across the industry include:

- ASC X12 v5010 997 Functional Acknowledgment (reports only ASC X12 standards syntax compliance and is not recommended by the ASC X12N Insurance Subcommittee to be used in health care)
- ASC X12C v5010 999 Implementation Acknowledgment (reports ASC X12C TR3 compliance errors and is recommended by the ASC X12N Insurance Subcommittee to be used in health care)
- ASC X12N v5010 277 Claim Acknowledgment (reports ONLY payer-specific business and ASC X12N v5010 837 Claim Technical Report Type 3 semantic editing results)
- Proprietary clearinghouse-specific or payer-specific reports

NOTE: The various ASC X12 standard acknowledgements identified have not been addressed or mandated by HIPAA at the present time.

CAQH CORE achieved substantial industry-wide consensus via its 2013 Industry Surveys that a Phase IV CAQH CORE 450 Health Care Claim (837) Infrastructure Rule should address the use of the ASC X12 standard acknowledgements specified in §3.2 below for the conduct of the HIPAA-mandated ASC X12N v5010 837 Claim transaction. CAQH CORE also agreed the requirements pertaining to acknowledgements in this Phase IV CAQH CORE 450 Health Care Claim (837) Infrastructure Rule be applicable only to:

- HIPAA-covered health plans or their agents receiving an ASC X12 Interchange of ASC X12N v5010 837 Claim transactions

And

- Receivers (defined in this CAQH CORE Operating Rule as HIPAA-covered providers or their agents) of any or all of the specified acknowledgements.

2.2 Real Time Adjudication

Real Time Claim Adjudication (RTA) relies on HIPAA-covered providers, HIPAA-covered health plans or all of their respective agents involved in the process to build Real Time connections to exchange claim transactions and respective acknowledgments, e.g., a rejection or confirmation that the claim has been successfully adjudicated and reimbursement will be forthcoming. An RTA process may include only the adjudication of a claim in Real Time with the actual claim payment processed at a later date. Alternatively, an RTA process may include both the adjudication of a claim and the actual payment of the claim. Whether claim payment is included in a HIPAA-covered health plan's RTA process is determined by each HIPAA-covered health plan.

Critical success factors for RTA include well-defined internal processes and governing policies of the respective providers and HIPAA-covered health plans (specific agreements regarding which claims for which beneficiaries can be submitted) as well as inter-enterprise standardization at the edge, i.e., the "rules-of-the-road". Such rules-of-the-road must address the unique and specific aspects for the Real Time exchange of claims and appropriate responses in a consistent, reliable manner that may be similar to but are uniquely different than simply applying to RTA the various CAQH CORE infrastructure requirements addressed in this Phase IV CAQH CORE 450 Health Care Claim (837) Infrastructure Rule. Simply because an ASC X12N v5010 837 Claim is submitted in Real Time does not then mean that the claim will be adjudicated in Real Time, either with or without Real Time claim payment.

NOTE: This Phase IV CAQH CORE 450 Health Care Claim (837) Infrastructure Rule does not address any requirements for RTA but does address certain requirements for when an ASC X12N v5010 837 Claim is submitted in Real Time without any adjudication. See Section 3.2.

3 Scope

3.1 What the Rule Applies To

This Phase IV CAQH CORE 450 Health Care Claim (837) Infrastructure Rule applies to the conduct of:

- ASC X12 Interchanges containing Functional Groups of any HIPAA-mandated ASC X12N v5010 837 Claim transaction
- ASC X12 Interchanges containing Functional Groups of any ASC X12N v5010 277CA Claim Acknowledgement transaction
- ASC X12 Interchanges containing Functional Groups of any ASC X12C v5010 999 Implementation Acknowledgement transaction

3.2 When the Rule Applies

This Phase IV CAQH CORE 450 Health Care Claim (837) Infrastructure Rule applies when:

- A HIPAA-covered health plan or its agent processes an ASC X12 Interchange containing one or more Functional Groups of one or more HIPAA-mandated ASC X12N v5010 837 Claim transactions submitted in Batch Processing Mode

Or

- A HIPAA-covered health plan or its agent processes an ASC X12 Interchange containing one or more Functional Groups of one or more HIPAA-mandated ASC X12N v5010 837 Claim transactions submitted in Real Time Processing Mode without Real Time adjudication

Or

- A HIPAA-covered entity receives:
    - An ASC X12C v5010 999 Implementation Acknowledgment of an ASC X12 Functional Group(s) of ASC X12N v5010 837 Claim transactions, or
    - An ASC X12N v5010 277CA transaction.

This rule **does not** apply:

- When the HIPAA-covered provider and the HIPAA-covered health plan are engaged in the conduct of Real Time Claim Adjudication (RTA)
- To the HIPAA-covered health plan-to-health plan or repricer exchange or routing of HIPAA-mandated ASC X12N v5010 837 Claim transactions

3.3 What the Rule Does Not Require

This rule does not require any entity to:

- Support the Real Time submission of ASC X12N v5010 837 Claim transactions (See Sections 4.1 and 4.4.1)
- Adjudicate in Real Time a claim or encounter submitted in Real Time
- Engage in the conduct of Real Time Claim Adjudication
- Integrate its current claims processing system components into its current eligibility or claim status processing system if they are not currently integrated

3.4 Outside the Scope of This Rule

The data content of any version of the following transactions is not addressed in this rule:

- ASC X12N v5010 277CA transaction
- ASC X12N v5010 837 Claim transaction
- ASC X12C v5010 999 transaction
- ASC X12 v5010 TA1 Interchange Acknowledgement transaction
- ASC X12N v5010 835 transaction.

3.5 Maintenance of This Rule

Should implementation of this rule be required via Federal regulation, any substantive updates to the rule (i.e., change to rule requirements) will be made in alignment with Federal processes for updating operating rule versions.

3.6 How the Rule Relates to CAQH CORE Phases I, II, and III

The Phase I CAQH CORE Eligibility/Benefits Operating Rules focused on improving Real Time electronic eligibility and benefits verification as eligibility is the first transaction in the claims process. The Phase II CAQH CORE Eligibility/Benefits and Claim Status Operating Rules focused on extending the value of electronic eligibility by adding additional data content requirements that deliver more robust patient financial liability information, including remaining deductibles, and adding more service type codes that must be supported. Building on this, CAQH CORE also determined that Phase II should be extended to include rules around the claim status transaction to allow providers to check electronically, in Real Time, the status of a claim without manual intervention or to confirm receipt of claims. Phase III was extended to include rules around the health care claim payment/advice transaction to allow the industry to leverage its investment in the Phase I and Phase II CAQH CORE Infrastructure Operating Rules.

This Phase IV rule adds to the Phase I, II, and III CAQH CORE infrastructure rule requirements by specifying the use of the ASC X12C v5010 999 transaction and the ASC X12N v5010 277CA transaction and other CAQH CORE infrastructure requirements when conducting any ASC X12N v5010 837 Claim transaction.

As with other CAQH CORE Operating Rules, general CAQH CORE policies also apply to Phase IV CAQH CORE Operating Rules and will be outlined in the Phase IV CAQH CORE Operating Rule Set.

This rule supports the CAQH CORE Guiding Principles that CAQH CORE Operating Rules will not be based on the least common denominator but rather will encourage feasible progress, and that CAQH CORE Operating Rules are a floor and not a ceiling, i.e., entities can go beyond the Phase IV CAQH CORE Operating Rules.

3.7 Assumptions

A goal of this rule is to adhere to the principles of electronic data interchange (EDI) in assuring that transactions sent are accurately received and to facilitate correction of errors for electronically submitted health care claims.

The following assumptions apply to this rule:

- A successful communication connection has been established.
- This rule is a component of the larger set of Phase IV CAQH CORE Operating Rules; as such, all of the CAQH CORE Guiding Principles apply to this rule and all other CAQH CORE Operating Rules.
- This rule is not a comprehensive companion document addressing any content requirements of any ASC X12N v5010 837 Claim transaction, the ASC X12C v5010 999 transaction, or the ASC X12N v5010 277CA transaction.
- Compliance with all CAQH CORE Operating Rules is a minimum requirement; any HIPAA-covered entity is free to offer more than what is required in the rule.

3.8 Abbreviations and Definitions Used in This Rule

Batch (Batch Mode, Batch Processing Mode)[7]: Batch Mode is when the initial (first) communications session is established and maintained open and active only for the time required to transfer a Batch file of one or more

[7] See Phase I CAQH CORE Glossary**:** http://www.caqh.org/sites/default/files/core/phase-i/reference/PIGlossary.pdf .

transactions. A separate (second) communications session is later established and maintained open and active for the time required to acknowledge that the initial file was successfully received and/or to retrieve transaction responses.

Batch Mode/Batch Processing Mode is also considered to be an asynchronous processing mode, whereby the associated messages are chronologically and procedurally decoupled. In a request-response interaction, the client agent can process the response at some indeterminate point in the future when its existence is discovered. Mechanisms to implement this capability may include: polling, notification by receipt of another message, receipt of related responses (as when the request receiver "pushes" the corresponding responses back to the requestor), etc.

Batch Mode/Batch Processing Mode is from the perspective of both the request initiator and the request responder. If a Batch (asynchronous) request is sent via intermediaries, then such intermediaries may, or may not, use Batch Processing Mode to further process the request.

Processing Mode: Refers to when the payload of the connectivity message envelope is processed by the receiving system, i.e., in Real Time or in Batch mode.

Real Time (Real Time Mode, Real Time Processing Mode)[8]: Real Time Mode is when an entity is required to send a transaction and receive a related response within a single communications session, which is established and maintained open and active until the required response is received by the entity initiating that session. Communication is complete when the session is closed.

Real Time Mode/Real Time Processing Mode is also considered to be a synchronous processing mode.

Real Time Mode/Real Time Processing Mode is from the perspective of both the request initiator and the request responder.

Safe Harbor: A "Safe Harbor" is generally defined as a statutory or regulatory provision that provides protection from a penalty or liability.[9]

In many IT-related initiatives, a safe harbor describes a set of standards/guidelines that allow for an "adequate" level of assurance when business partners are transacting business electronically.

The CAQH CORE Connectivity Safe Harbor requires the implementation of the CAQH CORE Connectivity Rule so that application vendors, HIPAA-covered providers, HIPAA-covered health plans or their respective agents can be assured the CAQH CORE Connectivity Rule will be supported by any trading partner. All entities must demonstrate the ability to implement connectivity as described in Phase IV CAQH CORE 470 Connectivity Rule v4.0.0.

4 Rule Requirements

4.1 Health Care Claim/Encounter Reporting Processing Mode Requirements

A HIPAA-covered health plan or its agent must implement the server requirements for Batch Processing Mode for the ASC X12N v5010 837 Claim transaction as specified in the Phase IV CAQH CORE 470 Connectivity Rule v4.0.0. Optionally, a HIPAA-covered health plan or its agent may elect to also implement the server requirements for Real Time Processing Modes as specified in the Phase IV CAQH CORE 470 Connectivity Rule v4.0.0.

The Phase IV CAQH CORE 470 Connectivity Rule v4.0.0 Real Time Processing Mode requirements are applicable when Real Time Processing Mode is offered for these transactions. The Phase IV CAQH CORE 470

[8] Ibid.
[9] Merriam-Webster's Dictionary of Law. Merriam-Webster, Inc., 28 May, 2007. <Dictionary.com http://dictionary.reference.com/browse/safeharbor>

Connectivity Rule v4.0.0 Batch Processing Mode requirements are applicable when Batch Processing Mode is offered for these transactions.

A HIPAA-covered health plan or its agent conducting the ASC X12N v5010 837 Claim transaction is required to conform to the processing mode requirements specified in this section regardless of any other connectivity modes and methods used between trading partners.

4.2 Health Care Claim Connectivity Requirements

A HIPAA-covered entity or its agent must be able to support the Phase IV CAQH CORE 470 Connectivity Rule v4.0.0.

This connectivity rule addresses usage patterns for Real Time and Batch Processing Modes, the exchange of security identifiers, and communications-level errors and acknowledgements. It does not attempt to define the specific content of the message payload exchanges beyond declaring the formats that must be used between entities and that security information must be sent outside of the message envelope payload.

All HIPAA-covered entities must demonstrate the ability to implement connectivity as described in the Phase IV CAQH CORE 470 Connectivity Rule v4.0.0. The Phase IV CAQH CORE 470 Connectivity Rule v4.0.0 is designed to provide a "Safe Harbor" that application vendors, HIPAA-covered providers and HIPAA-covered health plans (or other information sources) can be assured will be supported by any trading partner. Supported means that the entity is capable and ready at the time of the request by a trading partner to exchange data using the Phase IV CAQH CORE 470 Connectivity Rule v4.0.0. These requirements are not intended to require trading partners to remove existing connections that do not match the rule, nor are they intended to require that all trading partners must use this method for all new connections. CAQH CORE expects that in some technical circumstances, trading partners may agree to use different communication mechanism(s) and/or security requirements than those described by these requirements.

The requirement to support the Phase IV CAQH CORE 470 Connectivity Rule v4.0.0 does not apply to retail pharmacy. For retail pharmacy the entity should reference the NCPDP Connectivity Operating Rule v1.0 that can be obtained from www.ncpdp.org. NCPDP and CAQH CORE support a shared goal of continued alignment for connectivity across retail pharmacy and medical.

4.3 Health Care Claim/Encounter Reporting System Availability

Many healthcare providers have a need to submit health care claims and encounter reporting outside of the typical business day and business hours. Additionally, many institutional providers are now allocating staff resources to performing administrative and financial back-office activities on weekends and evenings. As a result, providers have a business need to be able to conduct health care claim and encounter reporting transactions at any time.

On the other hand, HIPAA-covered health plans have a business need to periodically take their claims processing and other systems offline in order to perform required system maintenance. This typically results in some systems not being available for timely processing of ASC X12N v5010 837 Claim, ASC X12C v5010 999, and ASC X12N v5010 277CA transactions on certain nights and weekends. This rule requirement addresses these conflicting needs.

4.3.1 System Availability Requirements

System availability must be no less than 86 percent per calendar week for both Real Time and Batch Processing Modes. System is defined as all necessary components required to process an ASC X12N v5010 837 Claim transaction, an ASC X12C v5010 999 transaction, and an X12N v5010 277CA transaction. Calendar week is defined as 12:01 a.m. Sunday to 12:00 a.m. the following Sunday. This will allow for a HIPAA-covered health

plan or its agent to schedule system updates to take place within a *maximum* of 24 hours per calendar week for regularly scheduled downtime.

4.3.2 Reporting Requirements

4.3.2.1 Scheduled Downtime

A HIPAA-covered health plan or its agent must publish its regularly scheduled system downtime in an appropriate manner (e.g., on websites or in Companion Guides) such that the HIPAA-covered health plan's trading partners can determine the health plan's system availability so that staffing levels can be effectively managed.

4.3.2.2 Non-Routine Downtime

For non-routine downtime (e.g., system upgrade), a HIPAA-covered health plan or its agent must publish the schedule of non-routine downtime at least one week in advance.

4.3.2.3 Unscheduled Downtime

For unscheduled/emergency downtime (e.g., system crash), a HIPAA-covered health plan or its agent are required to provide information within one hour of realizing downtime will be needed.

4.3.2.4 No Response Required

No response is required during scheduled, non-routine, or unscheduled downtime(s).

4.3.2.5 Holiday Schedule

Each HIPAA-covered health plan or its agent will establish its own holiday schedule and publish it in accordance with the rule requirements above.

4.4 Basic Requirements for a HIPAA-covered Health Plan or its Agent Receiving Electronic Claims/Encounter Reporting

4.4.1 Use of the 999 Implementation Acknowledgement and 277 Claim Acknowledgement

This rule section addresses the requirements for a HIPAA-covered health plan or its agent when it receives an ASC X12 Interchange containing one or more Functional Groups of any ASC X12N v5010 837 Claim transaction submitted either in Batch Processing Mode or in Real Time Processing Mode without Real Time Adjudication.

The requirements in this section do not apply to the conduct of a Real Time Adjudication (RTA) process in which a health care claim (ASC X12N v5010 837 Claim) is submitted to a HIPAA-covered health plan or its agent in Real Time and the HIPAA-covered health plan or its agent adjudicates that claim in Real Time during the same communications session and returns a single response to the submitter.

4.4.1.1 Functional Group and Transaction Set and Claim Acknowledgement

4.4.1.1.1 Requirements when any ASC X12 v5010 837 Claim Transaction is Submitted in Batch Processing Mode

When any Functional Group of any ASC X12N v5010 837 Claim Transaction Set is accepted, accepted with errors, or rejected the HIPAA-covered health plan or its agent must return a ASC X12C v5010 999 transaction.

The ASC X12C v5010 999 transaction must report each error detected to the most specific level of detail supported by the ASC X12N v5010 999 transaction.

A HIPAA-covered health plan or its agent must acknowledge each claim received in any Functional Group of any ASC X12N v5010 837 Claim Transaction Set using the ASC X12N v5010 277CA transaction only when ASC X12N v5010 837 Claim Transaction Set is not rejected.

NOTE: §1.4 Business Usage of the ASC X12N 277CA[10] transaction states that the "277 is the only notification of pre-adjudication claim status" and that "claims failing the pre-adjudication editing process are not forwarded to the claims adjudication system."

4.4.1.1.2 Requirements when any ASC X12N v5010 837 Claim Transaction is Submitted in Real Time Processing Mode without Adjudication

When any Functional Group of any ASC X12N v5010 837 Claim Transaction Set is rejected the HIPAA-covered health plan or its agent must return an ASC X12C v5010 999 transaction. The ASC X12C v5010 999 transaction must report each error detected to the most specific level of detail supported by the ASC X12N v5010 999 transaction.

An ASC X12C v5010 999 transaction must not be returned when the Functional Group of any ASC X12N v5010 837 Claim Transaction Set is not rejected.

A HIPAA-covered health plan or its agent must acknowledge each claim received in any Functional Group of any ASC X12N v5010 837 Claim Transaction Set using the ASC X12N v5010 277CA transaction only when ASC X12N v5010 837 Claim Transaction Set is accepted.

4.4.2 Response Time Requirements for Availability of Acknowledgements Addressed in this CAQH CORE Operating Rule

Maximum elapsed time for the availability of an ASC X12C v5010 999 transaction or ASC X12N v5010 277CA transaction to any ASC X12N v5010 837 Claim transaction that is submitted by a provider, or on a provider's behalf by a clearinghouse/switch, by 9:00 pm Eastern Time of a business day must be no later than 7:00 am Eastern Time the second business day following submission.

A business day consists of the 24 hours commencing with 12:00 am (Midnight or 0000 hours) of each designated day through 11:59 pm (2359 hours) of that same designated day. The actual calendar day(s) constituting business days are defined by and at the discretion of each HIPAA-covered health plan or its agent.

Each HIPAA-covered entity or its agent must support this *maximum* response time requirement to ensure that at least 90 percent of all required responses are returned within the specified maximum response time as measured within a calendar month.

Each HIPAA-covered entity or its agent must capture, log, audit, match, and report the date (YYYYMMDD), time (HHMMSS) and control numbers from its own internal systems and the corresponding data received from its trading partners.

Each HIPAA-covered entity or its agent must support these response time requirements in this section and other CAQH CORE Operating Rules regardless of the connectivity mode and methods used between trading partners.

[10] *ASC X12 005010X214 Health Care Claim Acknowledgement (277) Technical Report Type 3 Implementation Guide and associated errata*

4.5 Basic Requirements for Receivers of Acknowledgments

The receiver (defined in the context of this CAQH CORE Operating Rule as the HIPAA-covered provider or its agent) of an ASC X12C v5010 999 transaction and an ASC X12N v5010 277CA transaction is required:

- To process any ASC X12C v5010 999 transaction within one business day of its receipt

And

- To process any ASC X12N v5010 277CA transaction within one business day of its receipt

And

- To recognize all error conditions that can be specified using all standard acknowledgements named in this rule

And

- To pass all such error conditions to the end user as appropriate

Or

- To display to the end user text that uniquely describes the specific error condition(s), ensuring that the actual wording of the text displayed accurately represents the error code and the corresponding error description specified in the related ASC X12 acknowledgement specification without changing the meaning and intent of the error condition description.

The actual wording of the text displayed is at the discretion of the HIPAA-covered provider or its agent.

4.6 Health Care Claim Companion Guide

A HIPAA-covered health plan or its agent has the option of creating a "Companion Guide" that describes the specifics of how it will implement the HIPAA transactions. The Companion Guide is in addition to and supplements the ASC X12 TR3 Implementation Guide adopted for use under HIPAA.

Currently HIPAA-covered health plans or their agents have independently created Companion Guides that vary in format and structure. Such variance can be confusing to trading partners/providers who must review numerous Companion Guides along with the ASC X12 TR3 Implementation Guides. To address this issue, CAQH CORE developed the CAQH CORE v5010 Master Companion Guide Template for health plans or information sources. Using this template, health plans and information sources can ensure that the structure of their Companion Guide is similar to other health plan's documents, making it easier for providers to find information quickly as they consult each health plan's document on these important industry EDI transactions.

Developed with input from multiple health plans, system vendors, provider representatives, and health care/HIPAA industry experts, this template organizes information into several simple sections – General Information (Sections 1-9) and Transaction-Specific Information (Section 10) – accompanied by an appendix. Note that the Companion Guide template is presented in the form of an example from the viewpoint of a fictitious Acme Health Plan.

Although CAQH CORE believes that a standard template/common structure is desirable, it recognizes that different HIPAA-covered health plans may have different requirements. The CAQH CORE v5010 Master Companion Guide template gives health plans the flexibility to tailor the document to meet their particular needs.

The requirements specified in this section do not currently apply to retail pharmacy.

4.6.1 Health Care Claim Companion Guide Requirements

If a HIPAA-covered entity or its agent publishes a Companion Guide covering the ASC X12N v5010 837 Claim transaction then the Companion Guide must follow the format/flow as defined in the CAQH CORE v5010 Master Companion Guide Template for HIPAA Transactions (CAQH CORE v5010 Master Companion Guide Template available HERE). A HIPAA-covered entity or its agent's Companion Guide covering the ASC X12N v5010 837 Claim transaction must include the entity's requirements for coordination of benefits in Section 7 and Section 10 as appropriate.

NOTE: This rule does not require any HIPAA-covered entity to modify any other existing Companion Guides that cover other HIPAA-mandated transaction implementation guides.

5 Conformance Requirements

Conformance with this CAQH CORE Operating Rule can be voluntarily demonstrated and certified through successful completion of the Phase IV CAQH CORE Voluntary Certification Test Suite with a third party CAQH CORE-authorized Testing Vendor, followed by the entity's successful application for a CORE Certification Seal. A CORE Certification Seal demonstrates that an entity has successfully tested for conformity with all of the Phase IV CAQH CORE Operating Rules, and the entity or its product has fulfilled all relevant conformance requirements.

Only the Department of Health and Human Services (HHS) can decide whether a particular HIPAA-covered entity's system is **compliant** or **noncompliant** with the HIPAA Administrative Simplification requirements (which include HIPAA-adopted CAQH CORE Operating Rules). HHS may adjudicate on a HIPAA-covered entity's compliance and assess civil money penalties or penalty fees for noncompliance under the following HIPAA Administrative Simplification mandates:

- HIPAA regulations mandate that the Secretary "will impose a civil money penalty upon a covered entity or business associate if the Secretary determines that the covered entity or business associate has violated an administrative simplification provision." (47 CFR 160.402)
- Under the ACA, HIPAA mandates a certification process for HIPAA-covered health plans only, under which HIPAA-covered health plans are required to file a statement with HHS certifying that their data and information systems are in compliance with applicable standards and associated operating rules. (Social Security Act, Title XI, Section 1173(h)) HIPAA also mandates that a HIPAA-covered health plan must "ensure that any entities that provide services pursuant to a contact with such health plan shall comply with any applicable certification and compliance requirements." (Social Security Act, Title XI, Section 1173(h)(3))
- Under the ACA, HIPAA also mandates that HHS is to "conduct periodic audits to ensure that health plans…are in compliance with any standards and operating rules." (Social Security Act, Title XI, Section 1173(h))

6 Appendix

6.1 Appendix 1: References

- ASC X12C 005010X231 Implementation Acknowledgement for Health Care Insurance (999) Technical Report Type 3 Implementation Guide and associated errata
- ASC X12N 005010X222 Health Care Claim (837) Professional Technical Report Type 3 Implementation Guide and associated errata
- ASC X12N 005010X223 Health Care Claim (837) Institutional Technical Report Type 3 Implementation Guide and associated errata

- ASC X12N 005010X224 Health Care Claim (837) Dental Technical Report Type 3 Implementation Guide and associated errata
- ASC X12N 005010X214 Health Care Claim Acknowledgement (277) Technical Report Type 3 Implementation Guide and associated errata

Phase IV CAQH CORE Prior Authorization (278) Infrastructure Rule v4.1.0

February 2020

REVISION HISTORY FOR PHASE IV CAQH CORE PRIOR AUTHORIZATION (278) INFRASTRUCTURE RULE

Version	Revision	Description	Date
4.1.0	Major	Phase IV CAQH CORE Prior Authorization (278) Infrastructure Rule v4.1.0, balloted and approved by CAQH CORE Participating Organizations and CORE Board. Updates include: • Time requirement for health plan to request additional information/documentation • Time requirement for final determination (approval/denial) • Optional time requirement for a 5010X217 278 close out Additional non-substantive adjustments for clarity.	January 16, 2020

Table of Contents

1 Background Summary

Each Phase of CAQH CORE Operating Rules builds on the previous Phases to encourage feasible industry progress. Continuing to build on the Phase I, II, and III CAQH CORE Operating Rules, CAQH CORE determined that Phase IV should be extended to include rules around the health care services request for review and response transactions to allow the industry to leverage its investment in the Phase I, II, and III CAQH CORE infrastructure rules and apply them to conducting the X12/005010X217 Health Care Services Review – Request for Review and Response (278) transactions (hereafter referenced as "5010X217 278 Request and Response" and referred to as prior authorization in general) as well as the X12/005010X231 Implementation Acknowledgment for Health Care Insurance (999) and all associated errata hereafter referred to as "5010X231 999".

The 5010X217 278 Request and Response supports these key business events[11]:

- Admission certification review request and associated response
- Referral review request and associated response
- Health care services certification review request and associated response
- Extend certification review request and associated response
- Certification appeal review request and associated response
- Reservation of medical services request and associated response
- Cancellations of service reservations request and associated response

Benefits to the industry from applying the CAQH CORE infrastructure rules to prior authorization include:

- Increased consistency and automation across entities
- Increased electronic prior authorizations and a commensurate decrease in phone inquiries
- Reduced administrative costs
- More efficient processes
- Improved customer service to patients/subscribers
- Reduced staff time for phone inquiries
- Enhanced revenue cycle management
- Improved cash flow

The inclusion of this Phase IV CAQH CORE Operating Rule for the 5010X217 278 Request and Response continues to facilitate the industry's momentum to increase access to the HIPAA-mandated administrative transactions, and will encourage all HIPAA-covered entities, business associates, intermediaries, and vendors to build on and extend the infrastructure they have established for CAQH CORE Phases I, II, and III.

1.1 Affordable Care Act Mandates

This CAQH CORE Rule is part of a set of rules that addresses requirements in Section 1104 of the Affordable Care Act (ACA). Section 1104 contains an industry mandate for the use of operating rules to support implementation of the HIPAA standards. Using successful, yet voluntary, national industry efforts as a guide, Section 1104 defines operating rules as "the necessary business rules and guidelines for the

[11] X12/005010X217 Health Care Services Review – Request for Review and Response (278) Technical Report Type 3 Implementation Guide, Section 1.4.1.

electronic exchange of information that are not defined by a standard or its implementation specifications." As such, operating rules build upon existing healthcare transaction standards. The ACA outlines three sets of healthcare industry operating rules to be approved by the Department of Health and Human Services (HHS) and then implemented by the industry.

The third set of ACA-mandated operating rules address the health care claims or equivalent encounter information transactions, enrollment and disenrollment in a health plan, health plan premium payments, claims attachments, and referral certification and authorization.[12] The ACA requires HHS to adopt a set of operating rules for these five transactions by July 2014. [13] In a letter dated 09/12/12 to the Chairperson of the National Committee on Vital and Health Statistics (NCVHS),[14] the Secretary of HHS designated CAQH CORE as the operating rule authoring entity for the remaining five HIPAA-mandated electronic transactions.

Section 1104 of the ACA also adds the health claims attachment transaction to the list of electronic healthcare transactions for which the HHS Secretary must adopt a standard under HIPAA. The ACA requires the health claims attachment transaction standard to be adopted by 01/01/14, in a manner ensuring that it is effective by 01/01/16. [15]

NOTE: HHS has not adopted a standard for health claims attachments or indicated what standard(s) it might consider for the transaction, and an effective date for these operating rules is not included in the ACA. Thus, the immediate focus of the Phase IV CAQH CORE Operating Rules will not include attachments.

2 Issue to Be Addressed and Business Requirement Justification

When the HIPAA transactions were first mandated for use in October 2000[16], many HIPAA-covered health plan systems were not capable of processing the 5010X217 278 Request and Response transactions in Real Time. Usually, only Batch transactions were accepted. If Real Time transactions were accepted, the responses would not be returned in Real Time.

Even with the transition to v5010 in 2011, manual reviews still occur depending upon the complexity of the authorization and given many authorizations require supporting documentation. Although Batch processing of the 5010X217 278 Request facilitates the processing of certifications, referrals, admissions, and authorizations, etc., there is still a heavy reliance on manual processes within the HIPAA-covered health plan systems to generate a response. This manual process hinders broader adoption of the 5010X217 278 Request and Response transactions as the same information can be obtained more readily via phone or fax options already commonly used. While HIPAA-covered health plans have made much progress in accepting and responding to Real Time 5010X217 278 Requests and streamlining their manual processes, adoption of the HIPAA-mandated 5010X217 278 Request and Response still proves to be a challenge for many entities.

In addition to Batch only and manual processing of the 5010X217 278 Request and Response transactions, lack of product support for the 5010X217 278 Request and Response transactions also poses

[12] The first set of operating rules under ACA Section 1104 applies to eligibility and claim status transactions; these operating rules were effective 01/01/13. The second set of operating rules applies to EFT and ERA; these operating rules were effective 01/01/14.
[13] This date is statutory language and statutory language can be changed only by Congress.
[14] 09/12/12 HHS Letter from the Secretary to the Chairperson of NCVHS.
[15] These dates are statutory language and statutory language can be changed only by Congress.
[16] The first set of HIPAA-mandated transaction standards were adopted in the August 2000 HSS Final Rule, Health Insurance Reform: Standards for Electronic Transactions, with an effective date of October 16, 2000. This Final Rule adopted the ASC X12N 278 Health Care Services Review - Request for Review and Response as the standard for the referral certification and authorization transaction.

a challenge to greater industry adoption. Many vendors do not support this transaction within their practice management and patient accounting systems offerings. As such, providers are required to use the 5010X217 278 Request and Response submission tools that each HIPAA-covered health plan offers, often a web tool to submit the request. The development of vendor products for the submission and receipt of the 5010X217 278 Request and Response transactions is far behind the other HIPAA-mandated transactions and has hindered adoption of the 5010X217 278 Request and Response transactions across the industry.

By promoting consistent connectivity methods between HIPAA-covered providers and HIPAA-covered health plans, manual processes for requesting and receiving prior authorization can be reduced and electronic transaction usage increased. Defining acceptable acknowledgement response times, appropriate Batch and Real Time acknowledgements, system availability, and requiring entities that publish a Companion Guide do so in a common standard format to ensure that trading partners are informed of the nuances required for successful transaction processing will allow the industry to more easily adopt the 5010X217 278 Request and Response transactions.

In Phase I several CAQH CORE Infrastructure Operating Rules were approved that are designed to bring consistency and to improve the timely flow of the eligibility transactions. These infrastructure rules require:

- Real Time exchange of eligibility transactions within 20 seconds or less
- The consistent use of the 5010X231 999[17] for both Real Time and Batch exchanges
- 86% system availability of a HIPAA-covered health plan's eligibility processing system components over a calendar week
- Use of the public internet for connectivity
- Use of a best practices Companion Guide template for format and flow of Companion Guides for entities that issue them

In Phases II and III these CAQH CORE infrastructure rules were applied to the exchange of the HIPAA-mandated X12/005010X212 Health Care Claim Status Request and Response (276/277) transactions and the HIPAA-mandated X12/005010X221A1 Health Care Claim Payment/Advice (835) transaction. Phases II and III also included more robust, prescriptive, and comprehensive connectivity requirements.

During the Phase IV CAQH CORE rule development, CAQH CORE used discussion, research, and straw poll results to determine which infrastructure requirements should be applied to the exchange of the 5010X217 278 Request and Response transactions. Listed below is an overview of the infrastructure requirements incorporated into this rule in §4.

[17] The use of the ASC X12 TA1 Interchange Acknowledgement is not specifically addressed by the CAQH CORE Operating Rules. The A1 errata to Appendix C.1 of the ASC X12 999 provides industry guidance for the use of the TA1.

Phase IV Infrastructure Requirements for the 5010X217 278 Request and Response Transactions	
CAQH CORE Infrastructure Requirement Description	**Apply to Phase IV CAQH CORE Prior Authorization (278) Infrastructure Rule for the 5010X217 278 Request and Response**
Processing Mode*	**Y**
Connectivity	**Y**
System Availability	**Y**
Real Time Processing Mode Response Time	**Y**
Batch Processing Mode Response Time	**Y**
Real Time Acknowledgements	**Y**
Batch Acknowledgements	**Y**
Companion Guide	**Y**
***Note:** Beginning with Phase IV CAQH CORE Infrastructure Rules, processing mode requirements will be explicitly clarified. In previous phases this requirement was not as explicit as needed resulting in questions from implementers. The Phase IV CAQH CORE 470 Connectivity Rule v4.0.0 specifies the processing mode(s) that must be supported for each transaction addressed in Phase IV CAQH CORE Operating Rules.	

This Phase IV CAQH CORE Prior Authorization (278) Infrastructure Rule defines the specific requirements that HIPAA-covered health plans or their agents[18] and HIPAA-covered providers or their agents must satisfy. As with all CAQH CORE Operating Rules, these requirements are intended as a base or minimum set of requirements, and it is expected that many entities will go beyond these requirements as they work towards the goal of administrative interoperability. This Phase IV CAQH CORE Prior Authorization (278) Infrastructure Rule requires that HIPAA-covered health plans or their agents make appropriate use of the standard acknowledgements, support the CAQH CORE Connectivity requirements, and use the CAQH CORE v5010 Master Companion Guide Template when publishing their 5010X217 278 Companion Guide.

By applying these CAQH CORE infrastructure requirements to the conduct of the 5010X217 278 Request and Response transactions, this Phase IV CAQH CORE Prior Authorization (278) Infrastructure Rule helps provide the information that is necessary to electronically process a prior authorization request and thus reduce the current cost of today's manual transaction processes.

It is understood that applying the CAQH CORE infrastructure requirements to the exchange of the 5010X217 278 Request and Response transactions does not address the industry's transaction data content needs but rather establishes an electronic "highway". Subsequent phases of CAQH CORE rule-making may use the industry's experience and lessons learned from implementing the 5010X217 278 Request and Response transactions to develop a CAQH CORE Operating Rule addressing the data content of these transactions as various entities are testing content approaches.

[18] One who agrees and is authorized to act on behalf of another, a principal, to legally bind an individual in particular business transactions with third parties pursuant to an agency relationship. Source: West's Encyclopedia of American Law, edition 2. Copyright 2008 The Gale Group, Inc. All rights reserved.

2.1 Update to the Phase IV CAQH CORE Prior Authorization (278) Infrastructure Rule v4.1.0

Approved by CAQH CORE Participating Organizations and published in 2015, the response time requirement established in the initial version of the Phase IV CAQH CORE Prior Authorization (278) Infrastructure Rule represented a first step to setting national expectations for the completion of a prior authorization request and response exchange. Since then, industry commitment towards improving prior authorization response times only strengthened. A 2018 poll of CAQH CORE Participating Organizations indicated 73% participants supported pursuing development of additional response time requirements to build upon the Phase IV CAQH CORE Prior Authorization (278) Infrastructure Rule.

In response, CAQH CORE performed an extensive analysis of national and state-level prior authorization response time requirements and conducted interviews with a diverse mix of industry experts to understand the feasibility and impact of updating the existing response time requirement which, prior to this update, only specified a maximum timeframe for a health plan or its agent to return an initial 5010X217 278 Response – an approval, denial or pend.

From May 2019 through November 2019, the CAQH CORE Participating Organizations representing a diverse mix of provider, health plan, vendor and government representation convened to consider updates to the existing response time requirement. Participating Organizations completed impact assessments, straw polls, ballots, and participated in discussions to agree upon key response time enhancements. Ultimately, three key enhancements to the Phase IV CAQH CORE Prior Authorization (278) Infrastructure Rule were approved via the CAQH CORE Voting Process that enable timelier sending and receiving of batch and real time prior authorizations that are not urgent or emergent:

- Time requirement for health plan to request additional information/documentation
- Time requirement for final determination (approval/denial)
- Optional time requirement for a 5010X217 278 close out

As with all CAQH CORE Operating Rules, the response time requirements included in this update are a floor and not a ceiling, and health plans are encouraged to respond to prior authorization requests as quickly as possible to support patient care.

3 Scope

3.1 What the Rule Applies To

This Phase IV CAQH CORE Prior Authorization (278) Infrastructure Rule applies to the:

- X12/005010X217 Health Care Services Review – Request for Review and Response (278) Technical Report Type 3 and associated errata

And

- X12/005010X231 Implementation Acknowledgement for Health Care Insurance (999) Technical Report Type 3 and associated errata.

3.2 When the Rule Applies

This Phase IV CAQH CORE Prior Authorization (278) Infrastructure Rule applies when any HIPAA-covered entity or its agent uses, conducts, or processes the 5010X217 278 Request and Response transactions.

3.3 What the Rule Does Not Require

This rule does not require any entity or its agent to:

- Conduct, use, or process the 5010X217 278 Request and Response transactions if it currently does not do so or is not required by Federal or state regulation to do so.

3.4 Outside the Scope of This Rule

- This rule does not address any data content requirements of the 5010X217 278 Request and Response transactions. This Phase IV CAQH CORE Prior Authorization (278) Infrastructure Rule applicable to health care services review requests and responses is related to improving access to the transaction and **not to** addressing content requirements.
- Retail pharmacy benefit electronic prior authorizations are out of scope for this rule, i.e., pharmacist-and/or prescriber initiated prior authorization for drugs/biologics and other treatments covered under a pharmacy benefit.[19]
- Section 4.4 *Health Care Services Review – Request and Response Real Time Processing Mode Response Time Requirements* and Section 4.5 *Health Care Services Review – Request and Response Batch Processing Mode Response Time Requirements* do not apply to:
    1. Emergent[20] review request and associated responses.
    2. Urgent review request and associated responses.
    3. Review request and associated responses conducted retrospectively (i.e. neither prospectively[21] nor concurrently[22]).
    4. Review request and associated responses undergoing the Appeals Review Process (internal or external).

3.5 Maintenance of This Rule

Should implementation of this rule be required via Federal regulation, any substantive updates to the rule (i.e., change to rule requirements) will be made in alignment with Federal processes for updating versions of the operating rules.

3.6 How the Rule Relates to CAQH CORE Phases I, II, and III

The Phase I CAQH CORE Eligibility and Benefits Operating Rules focused on improving Real Time electronic eligibility and benefits verification as eligibility is the first transaction in the claims process. The Phase II CAQH CORE Eligibility/Benefits & Claim Status Operating Rules focused on extending the value of electronic eligibility by adding additional data content requirements that deliver more robust patient financial liability information, including remaining deductibles, and adding more service type codes that must be supported. Building on this, CAQH CORE also determined that Phase II should be extended to include infrastructure rules around the claim status transaction to allow providers to check electronically, in Real Time, the status of a claim, without manual intervention, or to confirm receipt of claims. Phase III was extended to include rules around the health care claim payment/advice transaction to allow the industry to leverage its investment in the Phase I and Phase II CAQH CORE Infrastructure Operating Rules.

---

[19] NCPDP is the Standards Setting Organization responsible for standards for retail pharmacy.
[20] The ACA prohibits requirements for prior authorization to access emergency services under section 29 CFR 2590.715-2719A, patient protections. In line with federal law, a growing number of state laws set additional limits around prior authorizations for emergency and urgent care.
[21] In the context of this CAQH CORE rule "prospective review" is defined as a utilization review conducted before an admission or a course of treatment including any required preauthorization or precertification, including extensions of outpatient treatment.
[22] In the context of this CAQH CORE rule "concurrent review" is defined as a utilization review conducted during a patient's hospital stay or course of inpatient treatment.

This Phase IV rule adds to the Phase I, II, and III CAQH CORE infrastructure rule requirements by specifying the use of the 5010X231 999 and the CAQH CORE infrastructure requirements when conducting the 5010X217 278 Request and Response transactions.

As with other CAQH CORE Operating Rules, general CAQH CORE policies also apply to Phase IV CAQH CORE Operating Rules and will be outlined in the Phase IV CAQH CORE Operating Rule Set.

This rule supports the CAQH CORE Guiding Principles that CAQH CORE Operating Rules will not be based on the least common denominator but rather will encourage feasible progress, and that CAQH CORE Operating Rules are a floor and not a ceiling, i.e., entities can go beyond the Phase IV CAQH CORE Operating Rules.

3.7 Assumptions

A goal of this rule is to adhere to the principles of electronic data interchange (EDI) in assuring that transactions sent are accurately received and to facilitate correction of errors for electronically submitted prior authorization requests.

The following assumptions apply to this rule:

- A successful communication connection has been established.
- This rule is a component of the larger set of Phase IV CAQH CORE Operating Rules; as such, all the CAQH CORE Guiding Principles apply to this rule and all other rules.
- This rule is not a comprehensive companion document addressing any content requirements of the 5010X217 278 Request and Response transactions or the 5010X231 999.
- Compliance with all CAQH CORE Operating Rules is a minimum requirement; any HIPAA-covered entity is free to offer more than what is required in the rule.

3.8 Abbreviations and Definitions Used in This Rule

Batch (Batch Mode, Batch Processing Mode)[23]**:** Batch Mode is when the initial (first) communications session is established and maintained open and active only for the time required to transfer a Batch file of one or more transactions. A separate (second) communications session is later established and maintained open and active for the time required to acknowledge that the initial file was successfully received and/or to retrieve transaction responses.

Batch Mode/Batch Processing Mode is also considered to be an asynchronous processing mode, whereby the associated messages are chronologically and procedurally decoupled. In a request-response interaction, the client agent can process the response at some indeterminate point in the future when its existence is discovered. Mechanisms to implement this capability may include: polling, notification by receipt of another message, receipt of related responses (as when the request receiver "pushes" the corresponding responses back to the requestor), etc.

Batch Mode/Batch Processing Mode is from the perspective of both the request initiator and the request responder. If a Batch (asynchronous) request is sent via intermediaries, then such intermediaries may, or may not, use Batch Processing Mode to further process the request.

Business Day: A business day consists of the 24 hours commencing with 12:00 am (Midnight or 0000 hours) of each designated day through 11:59 pm (2359 hours) of that same designated day. The actual

[23] See Phase I CAQH CORE Glossary**:** http://www.caqh.org/sites/default/files/core/phase-i/reference/PIGlossary.pdf.

calendar day(s) constituting business days are defined by and at the discretion of each HIPAA-covered health plan or its agent.

Processing Mode: Refers to when the payload of the connectivity message envelope is processed by the receiving system, i.e., in Real Time or in Batch mode.

Real Time (Real Time Mode, Real Time Processing Mode)[24]**:** Real Time Mode is when an entity is required to send a transaction and receive a related response within a single communications session, which is established and maintained open and active until the required response is received by the entity initiating that session. Communication is complete when the session is closed.

Real Time Mode/Real Time Processing Mode is also considered to be a synchronous processing mode.

Real Time Mode/Real Time Processing Mode is from the perspective of both the request initiator and the request responder.

Safe Harbor: A "Safe Harbor" is generally defined as a statutory or regulatory provision that provides protection from a penalty or liability.[25]

In many IT-related initiatives, a safe harbor describes a set of standards/guidelines that allow for an "adequate" level of assurance when business partners are transacting business electronically.

The CAQH CORE Connectivity Safe Harbor requires the implementation of the CAQH CORE Connectivity Rule so that application vendors, HIPAA-covered providers, HIPAA-covered health plans or their respective agents can be assured the CAQH CORE Connectivity Rule will be supported by any trading partner. All entities must demonstrate the ability to implement connectivity as described in Phase IV CAQH CORE 470 Connectivity Rule v4.0.0.

4 Rule Requirements

4.1 Health Care Services Review – Request and Response Processing Mode Requirements

A HIPAA-covered health plan or its agent must implement the server requirements for either Real Time Processing Mode **OR** Batch Processing Mode for the 5010X217 278 Request and Response transactions as specified in the Phase IV CAQH CORE 470 Connectivity Rule v4.0.0. Optionally, a HIPAA-covered health plan or its agent may elect to implement both Real Time and Batch Processing Modes.

The Phase IV CAQH CORE 470 Connectivity Rule v4.0.0 Real Time Processing Mode requirements are applicable when Real Time Processing Mode is offered for these transactions. The Phase IV CAQH CORE 470 Connectivity Rule v4.0.0 Batch Processing Mode requirements are applicable when Batch Processing Mode is offered for these transactions.

A HIPAA-covered health plan or its agent conducting the 5010X217 278 Request and Response transactions is required to conform to the processing mode requirements specified in this section regardless of any other connectivity modes and methods used between trading partners.

4.2 Health Care Services Review – Request and Response Connectivity Requirements

A HIPAA-covered entity or its agent must be able to support the Phase IV CAQH CORE 470 Connectivity Rule v4.0.0.

[24] Ibid.
[25] Merriam-Webster's Dictionary of Law. Merriam-Webster, Inc., 28 May, 2007. <Dictionary.com http://dictionary.reference.com/browse/safeharbor>

This connectivity rule addresses usage patterns for Real Time and Batch Processing Modes, the exchange of security identifiers, and communications-level errors and acknowledgements. It does not attempt to define the specific content of the message payload exchanges beyond declaring the formats that must be used between entities and that security information must be sent outside of the message envelope payload.

All HIPAA-covered entities must demonstrate the ability to implement connectivity as described in the Phase IV CAQH CORE 470 Connectivity Rule v4.0.0. The Phase IV CAQH CORE 470 Connectivity Rule v4.0.0 is designed to provide a "Safe Harbor" that application vendors, HIPAA-covered providers and HIPAA-covered health plans (or other information sources) can be assured will be supported by any trading partner. Supported means that the entity is capable and ready at the time of the request by a trading partner to exchange data using the Phase IV CAQH CORE 470 Connectivity Rule v4.0.0. These requirements are not intended to require trading partners to remove existing connections that do not match the rule, nor are they intended to require that all trading partners must use this method for all new connections. CAQH CORE expects that in some technical circumstances, trading partners may agree to use different communication mechanism(s) and/or security requirements than those described by these requirements.

4.3 Health Care Services Review – Request and Response System Availability

Many healthcare providers have a need to request prior authorizations outside of the typical business day and business hours. Additionally, many institutional providers are now allocating staff resources to performing administrative and financial back-office activities on weekends and evenings. As a result, providers have a business need to be able to conduct prior authorization transactions at any time.

On the other hand, HIPAA-covered health plans have a business need to periodically take their prior authorization processing and other systems offline in order to perform required system maintenance. This typically results in some systems not being available for timely processing of 5010X217 278 Request and Response and 5010X231 999 transactions on certain nights and weekends. This rule requirement addresses these conflicting needs.

4.3.1 System Availability Requirements

System availability must be no less than 86 percent per calendar week for both Real Time and Batch Processing Modes. System is defined as all necessary components required to process a 5010X217 278 Request and Response and a 5010X231 999 transaction. Calendar week is defined as 12:01 a.m. Sunday to 12:00 a.m. the following Sunday. This will allow for a HIPAA-covered health plan or its agent to schedule system updates to take place within a *maximum* of 24 hours per calendar week for regularly scheduled downtime.

4.3.2 Reporting Requirements

4.3.2.1 Scheduled Downtime

A HIPAA-covered health plan or its agent must publish its regularly scheduled system downtime in an appropriate manner (e.g., on websites or in Companion Guides) such that the HIPAA-covered health plan's trading partners can determine the health plan's system availability so that staffing levels can be effectively managed.

4.3.2.2 Non-Routine Downtime

For non-routine downtime (e.g., system upgrade), a HIPAA-covered health plan or its agent must publish the schedule of non-routine downtime at least one week in advance.

4.3.2.3 Unscheduled Downtime

For unscheduled/emergency downtime (e.g., system crash), a HIPAA-covered health plan or its agent are required to provide information within one hour of realizing downtime will be needed.

4.3.2.4 No Response Required

No response is required during scheduled, non-routine, or unscheduled downtime(s).

4.3.2.5 Holiday Schedule

Each HIPAA-covered health plan or its agent will establish its own holiday schedule and publish it in accordance with the rule requirements above.

4.4 Health Care Services Review – Request and Response Batch Processing Mode Response Time Requirements[26]

Each HIPAA-covered entity or its agent must support the *maximum* response time requirements to ensure that at least 90 percent of all required responses are returned within the specified maximum response times as measured within a calendar month.

Each HIPAA-covered entity or its agent must capture, log, audit, match, and report the date (YYYYMMDD), time (HHMMSS) and control numbers from its own internal systems and the corresponding data received from its trading partners.

Each HIPAA-covered entity or its agent must support the response time requirements in this section and other CAQH CORE Operating Rules regardless of the connectivity mode and methods used between trading partners.

4.4.1 5010X217 278 Initial Response Time Requirement (Batch Mode)

Maximum response time for availability of 5010X217 278 Responses when processing 5010X217 278 Requests submitted in Batch Processing Mode by a provider or on a provider's behalf by a clearinghouse/switch must be no later than the second business day following submission.

4.4.2 5010X231 999 Batch Processing Mode Response Time Requirement

A 5010X231 999 must be available to the submitter within one hour of receipt of the Batch:

- To the requester in the case of a Batch of 5010X217 278 Requests

And

- To the HIPAA-covered health plan or its agent in the case of a Batch of 5010X217 278 Responses.

4.4.3 Time Requirement for Requesting Additional Information/Documentation (Batch Mode)

When a health plan or its agent pends a 5010X217 278 Request due to a need for additional information/documentation from the provider or its agent, a health plan or its agent must make available a

[26] The Phase IV CAQH CORE Prior Authorization (278) Infrastructure Rule requires that a HIPAA-covered health plan or its agent must implement the server requirements for either Real Time Processing Mode OR Batch Processing Mode for the 5010X217 278 Request and Response transactions as specified in the Phase IV CAQH CORE 470 Connectivity Rule. Optionally, a HIPAA-covered health plan or its agent may elect to implement both Real Time and Batch Processing Modes.

5010X217 278 Response specifying what additional information/documentation is needed to reach a final determination within two business days following submission of the 5010X217 278 Request.

4.4.4 Time Requirement for Final Determination (Batch Mode)

Once a health plan or its agent receives a complete prior authorization request with all information and documentation necessary, including any peer to peer medical reviews conducted prior to a final determination[27], the health plan or its agent must return either a solicited or unsolicited 5010X217 278 Response containing an approval or denial within two business days following receipt of the completed prior authorization request.

4.5 Health Care Services Review – Request and Response Real Time Processing Mode Response Time Requirements

Each HIPAA-covered entity or its agent must support the *maximum* response time requirements to ensure that at least 90 percent of all required responses are returned within the specified maximum response times as measured within a calendar month.

Each HIPAA-covered entity or its agent must capture, log, audit, match, and report the date (YYYYMMDD), time (HHMMSS) and control numbers from its own internal systems and the corresponding data received from its trading partners.

Each HIPAA-covered entity or its agent must support these response time requirements in this section and other CAQH CORE Operating Rules regardless of the connectivity mode and methods used between trading partners.

4.5.1 Time Requirement for a 5010X217 278 Initial Response (Real Time Mode)

Maximum response time for the receipt of a 5010X217 278 Response from the time of submission of a 5010X217 278 Request must be 20 seconds when processing in Real Time Processing Mode. A 5010X231 999 response errors must be returned within 20 seconds.

The recommended maximum response time between each participant in the transaction routing path is 4 seconds or less per hop as long as the 20-second total roundtrip *maximum* requirement is met.

4.5.2 Time Requirement for Requesting Additional Information/Documentation when Known at Time of Request (Real Time Mode)

When a health plan or its agent pends a 5010X217 278 Request due to a need for additional information/documentation from the provider or its agent, and additional information/documentation necessary to complete the 5010X217 278 Request is immediately known by the health plan or its agent, the health plan or its agent must return the pended 5010X217 278 Response specifying what additional information/documentation is needed to reach a final determination within 20 seconds from the time of receipt of the 5010X217 278 Request. [28]

[27] Peer to peer medical reviews conducted after a final determination are a part of the appeals process, which is out of scope for this rule, per Section 3.4 *Outside the Scope of this Rule*.

[28] A health plan or its agent must communicate what additional information/documentation is needed to complete the PA request in real time if the health plan or its agent has a published policy that references the required documentation (e.g. companion guide, provider billing manuals, etc.).

4.5.3 Time Requirement for Requesting Additional Information/Documentation when Unknown at Time of Request (Real Time Mode)

After a health plan or its agent has pended the initial 5010X217 278 Request within 20 seconds from the time of submission due to a need for additional information/documentation, a health plan or its agent must return an unsolicited, 5010X217 278 Response specifying the additional information/documentation needed to reach a final determination within two business days of the initial 5010X217 278 Request[29].

4.5.4 Time Requirement for Final Determination after an Initial Pended Response (Real Time Mode)

After a health plan or its agent has sent an initial pended 5010X217 278 Response via Real Time Processing Mode, whether within 20 seconds in scenarios when additional information/documentation is immediately known or within two business days when additional information/documentation is not immediately known, a final determination must be sent via an unsolicited 5010X217 278 Response. Once a health plan or its agent receives a complete prior authorization request with all information and documentation necessary, including any peer to peer medical reviews conducted prior to the final determination[30], the health plan or its agent must return the unsolicited 5010X217 278 Response containing an approval or denial within two business days following receipt of the complete prior authorization request.

4.6 Health Care Services Review – Request and Response Request Close Out Requirement

4.6.1 Time Requirement for a 5010X217 278 Response Close Out Due to a Lack of Requested Information/Documentation

A health plan or its agent may choose to close out a 5010X217 278 Request if a provider or its agent does not respond to a request for additional information/documentation from the health plan or its agent after a minimum of 15 business days following the return of a pended 5010X217 278 Response requesting additional information/documentation necessary to adjudicate the pended 5010X217 278 Request.[31]

In the event a health plan or its agent determines to close out a 5010X217 278 Request due to non-receipt of requested additional information/documentation necessary to adjudicate the pended 5010X217 278 Request, the health plan or its agent must return an unsolicited 5010X217 278 Response communicating the prior authorization has been cancelled to the provider or its agent.

4.7 Health Care Services Review – Request and Response Real Time Acknowledgement Requirements

4.7.1 Use of the 5010X231 999 Implementation Acknowledgements for Real Time Processing Mode

A HIPAA-covered health plan or its agent must return:

---

[29] An unsolicited 5010X217 278 Response specifying what additional information/documentation is needed to reach a final determination is only required in cases when the health plan or its agent did not immediately know the information/documentation necessary and return that information with a solicited 5010X217 278 Response within 20 seconds. Therefore, Section 4.5.2 *Time Requirement for Requesting Additional Information/Documentation when Known at Time of Request* and Section 4.5.3 *Time Requirement for Requesting Additional Information/Documentation when Unknown at Time of Request* are mutually exclusive of one another.

[30] Peer to peer medical reviews conducted after a final determination are a part of the appeals process, which is out of scope for this rule, per Section 3.4 Outside the Scope of this Rule.

[31] A health plan or its agent should specify the processes for the close out and resubmission/appeal of a 5010X217 278 Response and any other provider notification in their Companion Guide, provider billing manual, or other organization policy manual to ensure business and technical processes are clearly articulated to its trading partner community.

- A 5010X231 999 to indicate that a Functional Group(s) or Transaction Set(s) is rejected.

A HIPAA-covered health plan or its agent must not return:

- A 5010X231 999 to indicate that a Functional Group(s) or Transaction Set(s) is accepted or accepted with errors.

Therefore, the submitter of a 5010X217 278 Request in Real Time will receive only one response from the HIPAA-covered health plan or its agent*: a 5010X231 999 rejection or a 5010X217 278 Response.*

4.8 Health Care Services Review – Request and Response Batch Acknowledgement Requirements

4.8.1 Use of the 5010X231 999 Implementation Acknowledgements for Batch Processing Mode

These requirements for use of the 5010X231 999 for Batch Processing Mode place parallel responsibilities on both requesters submitting the 5010X217 278 Request (i.e., providers or *their agents) and responders returning the 5010X217 278 Response (i.e.,* HIPAA-covered *health plans* or *their agents) for sending and accepting the 5010X231 999.* The goal of this approach is to adhere to the principles of EDI in assuring that transactions sent are accurately received and to facilitate correction of errors in Functional Groups of 5010X217 278 Requests and Functional Groups of 5010X217 278 Responses.

This rule assumes a successful communication connection has been established.

A HIPAA-covered entity or its agent must return a 5010X231 999 for each Functional Group of 5010X217 278 Request or 5010X217 278 Response transactions:

- To indicate that the Functional Group(s) was either accepted, accepted with errors, or rejected

And

- To specify for each included 5010X217 278 Request or 5010X217 278 Response Transaction Set that the transaction set was either accepted, accepted with errors, or rejected.

When a Functional Group of 5010X217 278 Request or a Functional Group of 5010X217 278 Response transactions is either accepted with errors or rejected, the 5010X231 999 must report each error detected to the most specific level of detail supported by the 5010X231 999.

4.9 Health Care Services Review – Request and Response Companion Guide

A HIPAA-covered health plan or its agent have the option of creating a "Companion Guide" that describes the specifics of how it will implement the HIPAA transactions. The Companion Guide is in addition to and supplements the ASC X12 TR3 Implementation Guide adopted for use under HIPAA.

Currently HIPAA-covered health plans or their agents have independently created Companion Guides that vary in format and structure. Such variance can be confusing to trading partners/providers who must review numerous Companion Guides along with the ASC X12 TR3 Implementation Guides. To address this issue, CAQH CORE developed the CAQH CORE v5010 Master Companion Guide Template for health plans or information sources. Using this template, health plans and information sources can ensure that the structure of their Companion Guide is similar to other health plan's documents, making it easier for providers to find information quickly as they consult each health plan's document on these important industry EDI transactions.

Developed with input from multiple health plans, system vendors, provider representatives, and health care/HIPAA industry experts, this template organizes information into several simple sections – General Information (Sections 1-9) and Transaction-Specific Information (Section 10) – accompanied by an appendix. Note that the Companion Guide template is presented in the form of an example from the viewpoint of a fictitious Acme Health Plan.

Although CAQH CORE believes that a standard template/common structure is desirable, it recognizes that different HIPAA-covered health plans may have different requirements. The CAQH CORE v5010 Master Companion Guide template gives health plans the flexibility to tailor the document to meet their particular needs.

The requirements specified in this section do not currently apply to retail pharmacy.

4.9.1 Health Care Services Review – Request and Response Companion Guide Requirements

If a HIPAA-covered entity or its agent publishes a Companion Guide covering the 5010X217 278 Request and Response transactions, the Companion Guide must follow the format/flow as defined in the CAQH CORE v5010 Master Companion Guide Template for HIPAA Transactions (CAQH CORE v5010 Master Companion Guide Template available HERE).

NOTE: This rule does not require any HIPAA-covered entity to modify any other existing Companion Guides that cover other HIPAA-mandated transaction implementation guides.

5 Conformance Requirements

Conformance with this CAQH CORE Operating Rule can be voluntarily demonstrated and certified through successful completion of the Phase IV CAQH CORE Voluntary Certification Test Suite with a third party CAQH CORE-authorized Testing Vendor, followed by the entity's successful application for a CORE Certification Seal. A CORE Certification Seal demonstrates that an entity has successfully tested for conformity with all of the Phase IV CAQH CORE Operating Rules, and the entity or its product has fulfilled all relevant conformance requirements.

Only the Department of Health and Human Services (HHS) can decide whether a particular HIPAA-covered entity's system is **compliant** or **noncompliant** with the HIPAA Administrative Simplification requirements (which include HIPAA-adopted CAQH CORE Operating Rules). HHS may adjudicate on a HIPAA-covered entity's compliance and assess civil money penalties or penalty fees for noncompliance under the following HIPAA Administrative Simplification mandates:

- HIPAA regulations mandate that the Secretary "will impose a civil money penalty upon a covered entity or business associate if the Secretary determines that the covered entity or business associate has violated an administrative simplification provision." (47 CFR 160.402)
- Under the ACA, HIPAA mandates a certification process for HIPAA-covered health plans only, under which HIPAA-covered health plans are required to file a statement with HHS certifying that their data and information systems are in compliance with applicable standards and associated operating rules. (Social Security Act, Title XI, Section 1173(h)) HIPAA also mandates that a HIPAA-covered health plan must "ensure that any entities that provide services pursuant to a contact with such health plan shall comply with any applicable certification and compliance requirements." (Social Security Act, Title XI, Section 1173(h)(3))

- Under the ACA, HIPAA also mandates that HHS is to "conduct periodic audits to ensure that health plans…are in compliance with any standards and operating rules." (Social Security Act, Title XI, Section 1173(h))

6 Appendix

6.1 Appendix 1: Reference

- X12/005010X231 Implementation Acknowledgement for Health Care Insurance (999) Technical Report Type 3 and associated errata
- X12/005010X217 Health Care Services Review – Request for Review and Response (278) Technical Report Type 3 Implementation Guide and associated errata

Phase IV CAQH CORE 454 Benefit Enrollment and Maintenance (834) Infrastructure Rule v4.0.0

September 2015

Table of Contents

1 Background Summary

Each Phase of CAQH CORE Operating Rules builds on the previous Phases to encourage feasible industry progress. Continuing to build on the Phase I, II, and III CAQH CORE Operating Rules, CAQH CORE determined that Phase IV should be extended to include rules around the benefit enrollment and maintenance transaction to allow the industry to leverage its investment in the Phase I, II, and III CAQH CORE infrastructure rules and apply them to conducting the ASC X12N 005010X220 Benefit and Enrollment Maintenance (834) transaction (hereafter referenced as ASC X12N v5010 834) as well as the ASC X12C 005010X231 Implementation Acknowledgment for Health Care Insurance (999) transaction and all associated errata (hereafter referred to as ASC X12C v5010 999). Benefits to the industry from applying the CAQH CORE infrastructure rules to the ASC X12N v5010 834 include:

- Increased consistency and automation across entities
- Reduced administrative costs
- More efficient processes
- Reduced staff time for phone inquiries
- Enhanced revenue cycle management

The inclusion of this Phase IV CAQH CORE Operating Rule for the ASC X12N v5010 834 continues to facilitate the industry's momentum to increase access to the HIPAA-mandated administrative transactions, and will encourage all HIPAA-covered entities, business associates, intermediaries, and vendors to build on and extend the infrastructure they have established for CAQH CORE Phases I, II, and III.

1.1 Affordable Care Act Mandates

This Phase IV CAQH CORE 454 Benefit Enrollment and Maintenance (834) Infrastructure Rule v4.0.0 is part of a set of rules that addresses requirements in Section 1104 of the Affordable Care Act (ACA). Section 1104 contains an industry mandate for the use of operating rules to support implementation of the HIPAA standards. Using successful, yet voluntary, national industry efforts as a guide, Section 1104 defines operating rules as "the necessary business rules and guidelines for the electronic exchange of information that are not defined by a standard or its implementation specifications." As such, operating rules build upon existing healthcare transaction standards. The ACA outlines three sets of healthcare industry operating rules to be approved by the Department of Health and Human Services (HHS) and then implemented by the industry.

The third set of ACA-mandated operating rules addresses the health care claims or equivalent encounter information transactions, enrollment and disenrollment in a health plan, health plan premium payments, claims attachments, and referral certification and authorization.[32] The ACA requires HHS to adopt a set of operating rules for these five transactions by July 2014.[33] In a letter dated 09/12/12 to the Chairperson of the National Committee on Vital and Health Statistics (NCVHS),[34] the Secretary of HHS designated CAQH CORE as the operating rule authoring entity for the remaining five HIPAA-mandated electronic transactions.

Section 1104 of the ACA also adds the health claims attachment transaction to the list of electronic healthcare transactions for which the HHS Secretary must adopt a standard under HIPAA. The ACA requires the health

[32] The first set of operating rules under ACA Section 1104 applies to eligibility and claim status transactions; these operating rules were effective 01/01/13. The second set of operating rules applies to EFT and ERA; these operating rules were effective 01/01/14.
[33] This date is statutory language and statutory language can be changed only by Congress.
[34] 09/12/12 HHS Letter from the Secretary to the Chairperson of NCVHS.

claims attachment transaction standard to be adopted by 01/01/14, in a manner ensuring that it is effective by 01/01/16[35].

NOTE: HHS has not adopted a standard for health claims attachments or indicated what standard(s) it might consider for the transaction, and an effective date for these operating rules is not included in the ACA. Thus, the immediate focus of the Phase IV CAQH CORE Operating Rules will not include attachments.

2 Issue to Be Addressed and Business Requirement Justification

When the HIPAA transactions were first mandated for use in October 2000[36], many health plan systems were not capable of processing the ASC X12N v4010 834 transaction in Real Time, thus only Batch transactions were accepted. If Real Time transactions were accepted, the responses would not be returned in Real Time.

Even with the transition to v5010 in 2011, the use of multiple connectivity methods and file formats still occurs depending upon the relationship between the health plan issuer and its trading partners. Results of straw polling conducted during development of this rule in 2014/2015 by the CAQH CORE Benefit Enrollment and Maintenance/Premium Payment Subgroup indicate the continued use of various file formats based on health plan issuer preference including manual processes.

By promoting consistent connectivity methods and the use of the HIPAA mandated transaction standard between health plan issuers and their trading partners, manual processes for benefit enrollment and maintenance can be reduced and electronic transaction usage increased. Defining acceptable use of response times, appropriate Batch and Real Time acknowledgements, system availability, and requiring entities that publish a Companion Guide do so in a common standard format to ensure that trading partners are informed of the nuances required for successful transaction processing will allow the industry to more easily adopt the ASC X12N v5010 834 transaction.

In Phase I several CAQH CORE Infrastructure Operating Rules were approved that are designed to bring consistency and to improve the timely flow of the eligibility transactions. These infrastructure rules require:

- Real Time exchange of eligibility transactions within 20 seconds or less
- The consistent use of the ASC X12C v5010 999[37] for both Real Time and Batch exchanges
- 86% system availability of a HIPAA-covered health plan's eligibility processing system components over a calendar week
- Use of the public internet for connectivity
- Use of a best practices Companion Guide template for format and flow of Companion Guides for entities that issue them

In Phases II and III these CAQH CORE infrastructure rules were applied to the exchange of the HIPAA-mandated ASC X12N 005010X212 Health Care Claim Status Request and Response (276/277) and the HIPAA-mandated ASC X12N 005010X221A1 Health Care Claim Payment/Advice (835) transactions. Phases II and III also included more robust, prescriptive, and comprehensive connectivity requirements.

[35] This date is statutory language and statutory language can be changed only by Congress.
[36] The first set of HIPAA-mandated transaction standards were adopted in the August 2000 HHS Final Rule, Health Insurance Reform: Standards for Electronic Transactions, with an effective date of October 16, 2000. A subsequent Final Rule published in January 2009 with an effective date of January 1, 2010, adopted the ASC X12N 005010X220 Benefit and Enrollment Maintenance (834) as the standard for the enrollment and disenrollment in a health plan.
[37] The use of the ASC X12 TA1 Interchange Acknowledgement is not specifically addressed by the CAQH CORE Operating Rules. The A1 errata to Appendix C.1 of the ASC X12 999 provides industry guidance for the use of the TA1.

During the Phase IV CAQH CORE rule development, CAQH CORE used discussion, research, and straw poll results to determine which infrastructure requirements should be applied to the exchange of the ASC X12N v5010 834 transaction. The table below lists the infrastructure requirements incorporated into this rule in §4.

Phase IV Infrastructure Requirements for the ASC X12N v5010 834 Transaction	
CAQH CORE Infrastructure Requirement Description	**Apply to Phase IV CAQH CORE Infrastructure Rule for the X12N v5010X220 834**
Processing Mode*	**Y**
Connectivity	**Y**
System Availability	**Y**
Real Time Processing Mode Response Time	**Y**
Batch Processing Mode Response Time	**Y**
Real Time Acknowledgements	**Y**
Batch Acknowledgements	**Y**
Companion Guide	**Y**
*__Note__: Beginning with Phase IV CAQH CORE Infrastructure Rules, processing mode requirements will be explicitly clarified. In previous phases this requirement was not as explicit as needed resulting in questions from implementers. The Phase IV CAQH CORE 470 Connectivity Rule v4.0.0 specifies the processing mode(s) that must be supported for each transaction addressed in Phase IV CAQH CORE Operating Rules.	

This Phase IV CAQH CORE 454 Benefit Enrollment and Maintenance (834) Infrastructure Rule defines the specific requirements that HIPAA-covered health plans or their agents[38] must satisfy. As with all CAQH CORE Operating Rules, these requirements are intended as a base or minimum set of requirements, and it is expected that many entities will go beyond these requirements as they work towards the goal of administrative interoperability. This Phase IV CAQH CORE 454 Benefit Enrollment and Maintenance (834) Infrastructure Rule requires that HIPAA-covered health plans or their agents make appropriate use of the standard acknowledgements, support the CAQH CORE Connectivity requirements, and use the CAQH CORE v5010 Master Companion Guide Template when publishing their ASC X12N v5010 834 Companion Guide.

By applying these CAQH CORE infrastructure requirements to the conduct of the ASC X12N v5010 834 transactions, this Phase IV CAQH CORE Benefit Enrollment and Maintenance (834) Infrastructure Rule helps provide the information that is necessary to electronically process a benefit enrollment or maintenance submission uniformly and consistently and thus reduce the cost of today's proprietary transaction processes.

It is understood that applying the CAQH CORE infrastructure requirements to the exchange of the ASC X12N v5010 834 transaction does not address the industry's transaction data content needs but rather establishes an electronic "highway". Subsequent phases of CAQH CORE rule-making may use the industry's experience and lessons learned from implementing the ASC X12N v5010 834 transaction to develop a CAQH CORE Operating Rule addressing the data content of these transactions as various entities are testing content approaches.

3 Scope

3.1 What the Rule Applies To

This Phase IV CAQH CORE 454 Benefit Enrollment and Maintenance (834) Infrastructure Rule v4.0.0 applies to the conduct of the HIPAA-mandated ASC X12N v5010 834 transaction.

[38] One who agrees and is authorized to act on behalf of another, a principal, to legally bind an individual in particular business transactions with third parties pursuant to an agency relationship. Source: West's Encyclopedia of American Law, edition 2. Copyright 2008 The Gale Group, Inc. All rights reserved.

3.2 When the Rule Applies

This Phase IV CAQH CORE 454 Benefit Enrollment and Maintenance (834) Infrastructure Rule v4.0.0 applies when a HIPAA-covered health plan or its agent uses, conducts, or processes the ASC X12N v5010 834 transaction.

3.3 What the Rule Does Not Require

This rule does not require any entity to conduct, use, or process the ASC X12N v5010 834 transaction if it currently does not do so or is not required by Federal or state regulation to do so.

3.4 Outside the Scope of This Rule

This rule does not address any data content requirements of the ASC X12N v5010 834 transaction. This Phase IV CAQH CORE 454 Benefit Enrollment and Maintenance (834) Infrastructure Rule v4.0.0 applicable to benefit enrollment and maintenance is related to improving access to the transaction and **not to** addressing content requirements.

This rule does not address requirements for the use of the ASC X12N v5010 834 transaction by the ACA Federal or state Health Information Exchanges (HIX).

3.5 Maintenance of This Rule

Should implementation of this rule be required via Federal regulation, any substantive updates to the rule (i.e., change to rule requirements) will be made in alignment with Federal processes for updating versions of the operating rules.

3.6 How the Rule Relates to CAQH CORE Phases I, II, and III

The Phase I CAQH CORE Eligibility/Benefits Operating Rules focused on improving Real Time electronic eligibility and benefits verification as eligibility is the first transaction in the claims process. The Phase II CAQH CORE Eligibility/Benefits & Claim Status Operating Rules focused on extending the value of electronic eligibility by adding additional data content requirements that deliver more robust patient financial liability information, including remaining deductibles, and adding more service type codes that must be supported. Building on this, CAQH CORE also determined that Phase II should be extended to include infrastructure rules around the claim status transaction to allow providers to check electronically, in Real Time, the status of a claim, without manual intervention, or to confirm receipt of claims. Phase III was extended to include rules around the health care claim payment/advice transaction to allow the industry to leverage its investment in the Phase I and Phase II CAQH CORE Infrastructure Operating Rules.

This Phase IV rule adds to the Phase I, II, and III CAQH CORE infrastructure rule requirements by specifying the use of the ASC X12C v5010 999 and the CAQH CORE infrastructure requirements when conducting the ASC X12N v5010 834 transaction.

As with other CAQH CORE Operating Rules, general CAQH CORE policies also apply to Phase IV CAQH CORE Operating Rules and will be outlined in the Phase IV CAQH CORE Operating Rule Set.

This rule supports the CAQH CORE Guiding Principles that CAQH CORE Operating Rules will not be based on the least common denominator but rather will encourage feasible progress, and that CAQH CORE Operating Rules are a floor and not a ceiling, i.e., entities can go beyond the Phase IV CAQH CORE Operating Rules.

3.7 Assumptions

A goal of this rule is to adhere to the principles of electronic data interchange (EDI) in assuring that transactions sent are accurately received and to facilitate correction of errors for electronically submitted benefit enrollment and maintenance transactions.

The following assumptions apply to this rule:

- A successful communication connection has been established.
- This rule is a component of the larger set of Phase IV CAQH CORE Operating Rules; as such, all the CAQH CORE Guiding Principles apply to this rule and all other rules.
- This rule is not a comprehensive companion document addressing any content requirements of the ASC X12N v5010 834 or the ASC X12C v5010 999 transactions.
- Compliance with all CAQH CORE Operating Rules is a minimum requirement; any entity is free to offer more than what is required in the rule.

3.8 Abbreviations and Definitions Used in This Rule

Batch (Batch Mode, Batch Processing Mode)[39]**:** Batch Mode is when the initial (first) communications session is established and maintained open and active only for the time required to transfer a batch file of one or more transactions. A separate (second) communications session is later established and maintained open and active for the time required to acknowledge that the initial file was successfully received and/or to retrieve transaction responses.

Batch Mode/Batch Processing Mode is also considered to be an asynchronous processing mode, whereby the associated messages are chronologically and procedurally decoupled. In a request-response interaction, the client agent can process the response at some indeterminate point in the future when its existence is discovered. Mechanisms to implement this capability may include: polling, notification by receipt of another message, receipt of related responses (as when the request receiver "pushes" the corresponding responses back to the requestor), etc.

Batch Mode/Batch Processing Mode is from the perspective of both the request initiator and the request responder. If a Batch (asynchronous) request is sent via intermediaries, then such intermediaries may, or may not, use Batch Processing Mode to further process the request.

Processing Mode: Refers to when the payload of the connectivity message envelope is processed by the receiving system, i.e., in Real Time or in Batch mode.

Real Time (Real Time Mode, Real Time Processing Mode)[40]**:** Real Time Mode is when an entity is required to send a transaction and receive a related response within a single communications session, which is established and maintained open and active until the required response is received by the entity initiating that session. Communication is complete when the session is closed.

Real Time Mode/Real Time Processing Mode is also considered to be a synchronous processing mode.

Real Time Mode/Real Time Processing Mode is from the perspective of both the request initiator and the request responder.

[39] Ibid.
[40] See Phase I CAQH CORE Glossary**:** http://www.caqh.org/sites/default/files/core/phase-i/reference/PIGlossary.pdf.

Safe Harbor: A "Safe Harbor" is generally defined as a statutory or regulatory provision that provides protection from a penalty or liability.[41]

In many IT-related initiatives, a safe harbor describes a set of standards/guidelines that allow for an "adequate" level of assurance when business partners are transacting business electronically.

The CAQH CORE Connectivity Safe Harbor requires the implementation of the Phase IV CAQH CORE 470 Connectivity Rule v4.0.0 so that application vendors, providers, and health plans (or other information sources) can be assured the CAQH CORE Connectivity Rule will be supported by any trading partner. All entities must demonstrate the ability to implement connectivity as described in Phase IV CAQH CORE 470 Connectivity Rule v4.0.0.

4 Rule Requirements

4.1 Benefit Enrollment and Maintenance Processing Mode Requirements

A HIPAA-covered health plan or its agent must implement the server requirements for Batch Processing Mode for the ASC X12N v5010 834 transaction as specified in the Phase IV CAQH CORE 470 Connectivity Rule v4.0.0. Optionally, a HIPAA-covered health plan or its agent may elect to implement the server requirements for Real Time Processing Mode for the ASC X12N v5010 834 transaction as specified in the Phase IV CAQH CORE 470 Connectivity Rule v4.0.0.

A HIPAA-covered health plan or its agent may also elect to implement the client requirements as specified in the Phase IV CAQH CORE 470 Connectivity Rule v4.0.0 in addition to implementing the server requirements. When a HIPAA-covered health plan or its agent elects to implement the client requirements as specified in the Phase IV CAQH CORE 470 Connectivity Rule v4.0.0 it must comply with all requirements specified in Sections 4.2, 4.3, 4.4, 4.5, 4.6, 5 and all respective Subsections.

The Phase IV CAQH CORE 470 Connectivity Rule v4.0.0 Real Time Processing Mode requirements are applicable when Real Time Processing Mode is offered for these transactions. The Phase IV CAQH CORE 470 Connectivity Rule v4.0.0 Batch Processing Mode requirements are applicable when Batch Processing Mode is offered for these transactions.

A HIPAA-covered health plan or its agent conducting the ASC X12N v5010 834 transaction is required to conform to the processing mode requirements specified in this section regardless of any other connectivity modes and methods used between trading partners.

4.2 Benefit Enrollment and Maintenance Connectivity Requirements

A HIPAA-covered entity or its agent must be able to support the Phase IV CAQH CORE 470 Connectivity Rule v4.0.0.

This connectivity rule addresses usage patterns for Real Time and Batch Processing Modes, the exchange of security identifiers, and communications-level errors and acknowledgements. It does not attempt to define the specific content of the message payload exchanges beyond declaring the formats that must be used between entities and that security information must be sent outside of the message envelope payload.

All HIPAA-covered entities must demonstrate the ability to implement connectivity as described in Phase IV CAQH CORE 470 Connectivity Rule v4.0.0. The Phase IV CAQH CORE 470 Connectivity Rule v4.0.0 is designed to provide a "Safe Harbor" that application vendors, providers and health plans or other entities can be

[41] Merriam-Webster's Dictionary of Law. Merriam-Webster, Inc., 28 May, 2007. <Dictionary.com http://dictionary.reference.com/browse/safeharbor>

assured will be supported by any trading partner. Supported means that the entity is capable and ready at the time of the request by a trading partner to exchange data using the Phase IV CAQH CORE 470 Connectivity Rule v4.0.0. These requirements are not intended to require trading partners to remove existing connections that do not match the rule, nor are they intended to require that all trading partners must use this method for all new connections. CAQH CORE expects that in some technical circumstances, trading partners may agree to use different communication mechanism(s) and/or security requirements than those described by these requirements.

4.3 Benefit Enrollment and Maintenance System Availability

Many health plan issuers and their trading partners have a need to conduct benefit enrollment and maintenance transactions outside of the typical business day and business hours. Additionally, health plan issuers and their trading partners are now allocating staff resources to performing administrative and financial back-office activities on weekends and evenings. As a result, health plan issuers and their trading partners have a business need to be able to conduct enrollment and disenrollment transactions at any time.

On the other hand, health plan issuers have a business need to periodically take their benefit enrollment and maintenance processing and other systems offline in order to perform required system maintenance. This typically results in some systems not being available for timely processing of ASC X12N v5010 834 and ASC X12C v5010 999 transactions on certain nights and weekends. This rule requirement addresses these conflicting needs.

4.3.1 System Availability Requirements

System availability must be no less than 86 percent per calendar week for both Real Time and Batch Processing Modes. System is defined as all necessary components required to process an ASC X12N v5010 834 and an ASC X12C v5010 999 transaction. Calendar week is defined as 12:01 a.m. Sunday to 12:00 a.m. the following Sunday. This will allow for a HIPAA-covered health plan or its agent to schedule system updates to take place within a *maximum* of 24 hours per calendar week for regularly scheduled downtime.

4.3.2 Reporting Requirements

4.3.2.1 Scheduled Downtime

A HIPAA-covered health plan or its agent must publish its regularly scheduled system downtime in an appropriate manner (e.g., on websites or in Companion Guides) such that the HIPAA-covered health plan's trading partners can determine the health plan’s system availability so that staffing levels can be effectively managed.

4.3.2.2 Non-Routine Downtime

For non-routine downtime (e.g., system upgrade), a HIPAA-covered health plan or its agent must publish the schedule of non-routine downtime at least one week in advance.

4.3.2.3 Unscheduled Downtime

For unscheduled/emergency downtime (e.g., system crash), a HIPAA-covered health plan or its agent are required to provide information within one hour of realizing downtime will be needed.

4.3.2.4 No Response Required

No response is required during scheduled, non-routine, or unscheduled downtime(s).

4.3.2.5 Holiday Schedule

Each HIPAA-covered health plan or its agent will establish its own holiday schedule and publish it in accordance with the rule requirements above.

4.4 Benefit Enrollment and Maintenance Real Time Processing Mode Response Time Requirements

Maximum response time for the receipt of an ASC X12C v5010 999 transaction from the time of submission of an ASC X12N v5010 834 must be 20 seconds when processing in Real Time Processing Mode.

Each HIPAA-covered entity or its agent must support this *maximum* response time requirement to ensure that at least 90 percent of all required responses are returned within the specified maximum response time as measured within a calendar month.

Each HIPAA-covered entity or its agent must capture, log, audit, match, and report the date (YYYYMMDD), time (HHMMSS) and control numbers from its own internal systems and the corresponding data received from its trading partners.

The recommended maximum response time between each participant in the transaction routing path is 4 seconds or less per hop as long as the 20-second total roundtrip *maximum* requirement is met.

Each HIPAA-covered entity or its agent must support these response time requirements in this section and other CAQH CORE Operating Rules regardless of the connectivity mode and methods used between trading partners.

The goal of this requirement is to adhere to the principles of EDI in assuring that transactions sent are accurately received and to facilitate correction of errors in Functional Groups of ASC X12N v5010 834 transactions.

This requirement assumes a successful communication connection has been established.

4.5 Benefit Enrollment and Maintenance Real Time Processing Mode Acknowledgement Requirements

A HIPAA-covered health plan or its agent must return an ASC X12C v5010 999 transaction to indicate that a Functional Group(s) or Transaction Set(s) is accepted, accepted with errors, or rejected and must report each error detected to the most specific level of detail supported by the ASC X12C v5010 999 transaction.

4.6 Benefit Enrollment and Maintenance Batch Processing Mode Response Time Requirements

Maximum response time for availability of ASC X12C v5010 999 transaction when processing an ASC X12N v5010 834 transaction submitted in Batch Processing Mode by 9:00 pm Eastern Time of a business day by a health plan sponsor or its agent must be no later than 7:00 am Eastern Time the third business day following submission.

A business day consists of the 24 hours commencing with 12:00 am (Midnight or 0000 hours) of each designated day through 11:59 pm (2359 hours) of that same designated day. The actual calendar day(s) constituting business days are defined by and at the discretion of each HIPAA-covered health plan or its agent.

Each HIPAA-covered entity or its agent must support this *maximum* response time requirement to ensure that at least 90 percent of all required responses are returned within the specified maximum response time as measured within a calendar month.

Each HIPAA-covered entity or its agent must capture, log, audit, match, and report the date (YYYYMMDD), time (HHMMSS) and control numbers from its own internal systems and the corresponding data received from its trading partners.

Each HIPAA-covered entity or its agent must support these response time requirements in this section and other CAQH CORE Operating Rules regardless of the connectivity mode and methods used between trading partners.

The goal of this requirement is to adhere to the principles of EDI in assuring that transactions sent are accurately received and to facilitate correction of errors in Functional Groups of ASC X12N v5010 834 transactions.

This requirement assumes a successful communication connection has been established.

4.7 Benefit Enrollment and Maintenance Batch Processing Mode Acknowledgement Requirements

A HIPAA-covered health plan or its agent must return an ASC X12C v5010 999 transaction for each Functional Group of ASC X12N v5010 834 transactions:

- To indicate that the Functional Group(s) was either accepted, accepted with errors, or rejected

And

- To specify for each included ASC X12N v5010 834 that the transaction set was either accepted, accepted with errors, or rejected.

The HIPAA-covered health plan or its agent must not return the ASC X12C v5010 999 transaction during the initial communications session in which the ASC X12N v5010 834 transaction is submitted.

When a Functional Group of ASC X12N v5010 834 of transactions is either accepted with errors or rejected, the ASC X12C v5010 999 transaction must report each error detected to the most specific level of detail supported by the ASC X12C v5010 999 transaction.

4.8 Elapsed Time for Enrollment System Processing of Received Benefit Enrollment Data

A HIPAA-covered health plan or its agent must process the benefit enrollment and maintenance data by its enrollment application system within five business days following the successful receipt and validation of the data. In the context of this rule

- *Successful Receipt* means that the ASC X12N v5010 834 transaction has not been rejected by the health plan or its agent's EDI management system

And

- *Validation* means that any data inconsistencies detected in an accepted ASC X12N v5010 834 transaction which would prevent accurate posting of that data to the health plan or its agent's internal enrollment application system have been resolved.

4.9 Benefit Enrollment and Maintenance Companion Guide

A HIPAA-covered health plan or its agent has the option of creating a "Companion Guide" that describes the specifics of how it will implement the HIPAA transactions. The Companion Guide is in addition to and supplements the ASC X12 TR3 Implementation Guide adopted for use under HIPAA.

Currently HIPAA-covered health plans or their agents have independently created Companion Guides that vary in format and structure. Such variance can be confusing to trading partners who must review numerous Companion Guides along with the ASC X12 TR3 Implementation Guides. To address this issue, CAQH CORE developed the CAQH CORE v5010 Master Companion Guide Template for health plans or their agents. Using this template, health plans or their agents can ensure that the structure of their Companion Guide is similar to other health plan's documents, making it easier for its trading partners to find information quickly as they consult each health plan's document on these important industry EDI transactions.

Developed with input from multiple health plans, system vendors, provider representatives, and health care/HIPAA industry experts, this template organizes information into several simple sections – General Information (Sections 1-9) and Transaction-Specific Information (Section 10) – accompanied by an appendix.

Note that the Companion Guide template is presented in the form of an example from the viewpoint of a fictitious Acme Health Plan.

Although CAQH CORE believes that a standard template/common structure is desirable, it recognizes that different health plans may have different requirements. The CAQH CORE v5010 Master Companion Guide template gives health plans the flexibility to tailor the document to meet their particular needs.

4.9.1 Benefit Enrollment and Maintenance Companion Guide Requirements

If a HIPAA-covered entity or its agent publishes a Companion Guide covering the ASC X12N v5010 834 transaction, the Companion Guide must follow the format/flow as defined in the CAQH CORE v5010 Master Companion Guide Template for HIPAA Transactions (CAQH CORE v5010 Master Companion Guide Template available HERE).

NOTE: This rule does not require any entity to modify any other existing Companion Guides that cover other HIPAA-mandated transaction implementation guides.

5 Conformance Requirements

Conformance with this CAQH CORE Operating Rule can be voluntarily demonstrated and certified through successful completion of the Phase IV CAQH CORE Voluntary Certification Test Suite with a third party CAQH CORE-authorized Testing Vendor, followed by the entity's successful application for a CORE Certification Seal. A CORE Certification Seal demonstrates that an entity has successfully tested for conformity with all of the Phase IV CAQH CORE Operating Rules, and the entity or its product has fulfilled all relevant conformance requirements.

Only the Department of Health and Human Services (HHS) can decide whether a particular HIPAA-covered entity's system is **compliant** or **noncompliant** with the HIPAA Administrative Simplification requirements (which include HIPAA-adopted CAQH CORE Operating Rules). HHS may adjudicate on a HIPAA-covered entity's compliance and assess civil money penalties or penalty fees for noncompliance under the following HIPAA Administrative Simplification mandates:

- HIPAA regulations mandate that the Secretary "will impose a civil money penalty upon a covered entity or business associate if the Secretary determines that the covered entity or business associate has violated an administrative simplification provision." (47 CFR 160.402)
- Under the ACA, HIPAA mandates a certification process for HIPAA-covered health plans only, under which HIPAA-covered health plans are required to file a statement with HHS certifying that their data and information systems are in compliance with applicable standards and associated operating rules. (Social Security Act, Title XI, Section 1173(h)) HIPAA also mandates that a HIPAA-covered health plan must "ensure that any entities that provide services pursuant to a contact with such health plan shall comply with any applicable certification and compliance requirements." (Social Security Act, Title XI, Section 1173(h)(3))
- Under the ACA, HIPAA also mandates that HHS is to "conduct periodic audits to ensure that health plans…are in compliance with any standards and operating rules." (Social Security Act, Title XI, Section 1173(h))

6 Appendix

6.1 Appendix 1: Reference

- ASC X12C 005010X231 Implementation Acknowledgement for Health Care Insurance (999) Technical Report Type 3 and associated errata
- ASC X12N 005010X220 Benefit Enrollment and Maintenance (834) Technical Report Type 3 Implementation Guide and associated errata

Phase IV CAQH CORE 456 Payroll Deducted and Other Group Premium Payment for Insurance Products (820) Infrastructure Rule v4.0.0

September 2015

Table of Contents

1 Background Summary

Each Phase of CAQH CORE Operating Rules builds on the previous Phases to encourage feasible industry progress. Continuing to build on the Phase I, II, and III CAQH CORE Operating Rules, CAQH CORE determined that Phase IV should be extended to include rules around the health plan premium payment transaction to allow the industry to leverage its investment in the Phase I, II, and III CAQH CORE infrastructure rules and apply them to conducting the ASC X12N 005010X218 Payroll Deducted and Other Group Premium Payment for Insurance Products (820) transaction (hereafter referenced as ASC X12N v5010 820) as well as the ASC X12C 005010X231 Implementation Acknowledgment for Health Care Insurance (999) transaction and all associated errata (hereafter referred to as ASC X12C v5010 999.) Benefits to the industry from applying the CAQH CORE infrastructure rules to the ASC X12N v5010 820 transaction include:

- Increased consistency and automation across entities
- Reduced administrative costs
- More efficient processes
- Reduced staff time for phone inquiries
- Enhanced revenue cycle management

The inclusion of this Phase IV CAQH CORE Operating Rule for the ASC X12N v5010 820 transaction continues to facilitate the industry's momentum to increase access to the HIPAA-mandated administrative transactions, and will encourage all HIPAA-covered entities, business associates, intermediaries, and vendors to build on and extend the infrastructure they have established for CAQH CORE Phases I, II, and III.

1.1 Affordable Care Act Mandates

This Phase IV CAQH CORE 456 Payroll Deducted and Other Group Premium Payment for Insurance Products (820) Infrastructure Rule v4.0.0 is part of a set of rules that addresses requirements in Section 1104 of the Affordable Care Act (ACA). Section 1104 contains an industry mandate for the use of operating rules to support implementation of the HIPAA standards. Using successful, yet voluntary, national industry efforts as a guide, Section 1104 defines operating rules as "the necessary business rules and guidelines for the electronic exchange of information that are not defined by a standard or its implementation specifications." As such, operating rules build upon existing healthcare transaction standards. The ACA outlines three sets of healthcare industry operating rules to be approved by the Department of Health and Human Services (HHS) and then implemented by the industry.

The third set of ACA-mandated operating rules addresses the health care claims or equivalent encounter information transactions, enrollment and disenrollment in a health plan, health plan premium payments, claims attachments, and referral certification and authorization.[42] The ACA requires HHS to adopt a set of operating rules for these five transactions by July 2014.[43] In a letter dated 09/12/12 to the Chairperson of the National Committee on Vital and Health Statistics (NCVHS),[44] the Secretary of HHS designated CAQH CORE as the operating rule authoring entity for the remaining five HIPAA-mandated electronic transactions.

Section 1104 of the ACA also adds the health claims attachment transaction to the list of electronic healthcare transactions for which the HHS Secretary must adopt a standard under HIPAA. The ACA requires the health

[42] The first set of operating rules under ACA Section 1104 applies to eligibility and claim status transactions; these operating rules were effective 01/01/13. The second set of operating rules applies to EFT and ERA; these operating rules were effective 01/01/14.
[43] This date is statutory language and statutory language can be changed only by Congress.
[44] 09/12/12 HHS Letter from the Secretary to the Chairperson of NCVHS.

claims attachment transaction standard to be adopted by 01/01/14, in a manner ensuring that it is effective by 01/01/16[45].

NOTE: HHS has not adopted a standard for health claims attachments or indicated what standard(s) it might consider for the transaction, and an effective date for these operating rules is not included in the ACA. Thus, the immediate focus of the Phase IV CAQH CORE Operating Rules will not include attachments.

2 Issue to Be Addressed and Business Requirement Justification

When the HIPAA transactions were first mandated for use in October 2000[46], many health plan systems were not capable of processing the ASC X12N v4010 820 transactions in Real Time, thus only Batch transactions were accepted. If Real Time transactions were accepted, the responses would not be returned in Real Time.

Even with the transition to v5010 in 2011, the use of multiple connectivity methods and file formats still occurs depending upon the relationship between the health plan issuer and its trading partners. Results of straw polling conducted during development of this rule in 2014/2015 by the CAQH CORE Benefit Enrollment and Maintenance/Premium Payment Subgroup indicate the continued use of various file formats based on health plan issuer preference including manual processes.

By promoting consistent connectivity methods and the use of the HIPAA mandated transaction standard between health plan issuers and their trading partners, manual processes for Payroll Deducted and Other Group Premium Payment for Insurance Products can be reduced and electronic transaction usage increased. Defining acceptable use of response times, appropriate Batch and Real Time acknowledgements, system availability, and requiring entities that publish a Companion Guide do so in a common standard format to ensure that trading partners are informed of the nuances required for successful transaction processing will allow the industry to more easily adopt the ASC X12N v5010 820 transaction.

In Phase I several CAQH CORE Infrastructure Operating Rules were approved that are designed to bring consistency and to improve the timely flow of the eligibility transactions. These infrastructure rules require:

- Real Time exchange of eligibility transactions within 20 seconds or less
- The consistent use of the ASC X12C v5010 999[47] for both Real Time and Batch exchanges
- 86% system availability of a HIPAA-covered health plan's eligibility processing system components over a calendar week
- Use of the public internet for connectivity
- Use of a best practices Companion Guide template for format and flow of Companion Guides for entities that issue them

In Phases II and III these CAQH CORE infrastructure rules were applied to the exchange of the HIPAA-mandated ASC X12 005010X212 Health Care Claim Status Request and Response (276/277) and the HIPAA-mandated ASC X12N 005010X221A1 Health Care Claim Payment/Advice (835) transactions. Phases II and III also included more robust, prescriptive, and comprehensive connectivity requirements.

---

[45] This date is statutory language and statutory language can be changed only by Congress.

[46] The first set of HIPAA-mandated transaction standards were adopted in the August 2000 HHS Final Rule, Health Insurance Reform: Standards for Electronic Transactions, with an effective date of October 16, 2000. A subsequent Final Rule published in January 2009 with an effective date of January 1, 2010, adopted the ASC X12N 005010X218 Payroll Deducted and Other Group Premium Payment for Insurance Products (820) as the standard for the payment of health plan premiums.

[47] The use of the ASC X12 TA1 Interchange Acknowledgement is not specifically addressed by the CAQH CORE Operating Rules. The A1 errata to Appendix C.1 of the ASC X12 999 provides industry guidance for the use of the TA1.

During the Phase IV CAQH CORE rule development, CAQH CORE used discussion, research, and straw poll results to determine which infrastructure requirements should be applied to the exchange of the ASC X12N v5010 820 transaction. The table below lists the infrastructure requirements incorporated into this rule in §4.

Phase IV Infrastructure Requirements for the ASC X12N v5010 820 Transaction	
CAQH CORE Infrastructure Requirement Description	**Apply to Phase IV CAQH CORE Infrastructure Rule for the X12N v5010X218 820**
Processing Mode*	**Y**
Connectivity	**Y**
System Availability	**Y**
Real Time Processing Mode Response Time	**Y**
Batch Processing Mode Response Time	**Y**
Real Time Acknowledgements	**Y**
Batch Acknowledgements	**Y**
Companion Guide	**Y**
*__Note__: Beginning with Phase IV CAQH CORE Infrastructure Rules, processing mode requirements will be explicitly clarified. In previous phases this requirement was not as explicit as needed resulting in questions from implementers. The Phase IV CAQH CORE 470 Connectivity Rule v4.0.0 specifies the processing mode(s) that must be supported for each transaction addressed in Phase IV CAQH CORE Operating Rules.	

This Phase IV CAQH CORE 456 Payroll Deducted and Other Group Premium Payment for Insurance Products (820) Infrastructure Rule v4.0.0 defines the specific requirements that HIPAA-covered health plans or their agents[48] must satisfy. As with all CAQH CORE Operating Rules, these requirements are intended as a base or minimum set of requirements, and it is expected that many entities will go beyond these requirements as they work towards the goal of administrative interoperability. This Phase IV CAQH CORE 456 Payroll Deducted and Other Group Premium Payment for Insurance Products (820) Infrastructure Rule v4.0.0 requires that HIPAA-covered health plans or their agents make appropriate use of the standard acknowledgements, support the CAQH CORE Connectivity requirements, and use the CAQH CORE v5010 Master Companion Guide Template when publishing their ASC X12N v5010 820 Companion Guide.

By applying these CAQH CORE infrastructure requirements to the conduct of the ASC X12N v5010 820 transactions, this Phase IV CAQH CORE Payroll Deducted and Other Group Premium Payment for Insurance Products (820) Infrastructure Rule v4.0.0 helps provide the information that is necessary to electronically process a premium payment remittance advice uniformly and consistently and thus reduce the cost of today's proprietary transaction processes.

It is understood that applying the CAQH CORE infrastructure requirements to the exchange of the ASC X12N v5010 820 transaction does not address the industry's transaction data content needs but rather establishes an electronic "highway". Subsequent phases of CAQH CORE rule-making may use the industry's experience and lessons learned from implementing the ASC X12N v5010 820 transaction to develop a CAQH CORE Operating Rule addressing the data content of these transactions as various entities are testing content approaches.

[48] One who agrees and is authorized to act on behalf of another, a principal, to legally bind an individual in particular business transactions with third parties pursuant to an agency relationship. Source: West's Encyclopedia of American Law, edition 2. Copyright 2008 The Gale Group, Inc. All rights reserved.

3 Scope

3.1 What the Rule Applies To

This Phase IV CAQH CORE 456 Payroll Deducted and Other Group Premium Payment for Insurance Products (820) Infrastructure Rule v4.0.0 applies to the conduct of the HIPAA-mandated ASC X12N v5010 820 transaction.

3.2 When the Rule Applies

This Phase IV CAQH CORE 456 Payroll Deducted and Other Group Premium Payment for Insurance Products (820) Infrastructure Rule v4.0.0 applies when a HIPAA-covered health plan or its agent uses, conducts, or processes the ASC X12N v5010 820 transaction.

3.3 What the Rule Does Not Require

This rule does not require any entity to conduct, use, or process the ASC X12N v5010 820 transaction if it currently does not do so or is not required by Federal or state regulation to do so.

3.4 Outside the Scope of This Rule

This rule does not address any data content requirements of the ASC X12N v5010 820 transaction. This Phase IV CAQH CORE 456 Payroll Deducted and Other Group Premium Payment for Insurance Products (820) Infrastructure Rule v4.0.0 applicable to health plan premium payment is related to improving access to the transaction and **not to** addressing content requirements.

This rule does not address requirements for the use of the ASC X12N v5010 820 transaction by the ACA Federal or state Health Information Exchanges (HIX).

3.5 Maintenance of This Rule

Should implementation of this rule be required via Federal regulation, any substantive updates to the rule (i.e., change to rule requirements) will be made in alignment with Federal processes for updating versions of the operating rules.

3.6 How the Rule Relates to CAQH CORE Phases I, II, and III

The Phase I CAQH CORE Eligibility/Benefits Operating Rules focused on improving Real Time electronic eligibility and benefits verification as eligibility is the first transaction in the claims process. The Phase II CAQH CORE Eligibility/Benefits & Claim Status Operating Rules focused on extending the value of electronic eligibility by adding additional data content requirements that deliver more robust patient financial liability information, including remaining deductibles, and adding more service type codes that must be supported. Building on this, CAQH CORE also determined that Phase II should be extended to include infrastructure rules around the claim status transaction to allow providers to check electronically, in Real Time, the status of a claim, without manual intervention, or to confirm receipt of claims. Phase III was extended to include rules around the health care claim payment/advice transaction to allow the industry to leverage its investment in the Phase I and Phase II CAQH CORE Infrastructure Operating Rules.

This Phase IV rule adds to the Phase I, II, and III CAQH CORE infrastructure rule requirements by specifying the use of the ASC X12C v5010 999 and the CAQH CORE infrastructure requirements when conducting the ASC X12N v5010 820 transaction.

As with other CAQH CORE Operating Rules, general CAQH CORE policies also apply to Phase IV CAQH CORE Operating Rules and will be outlined in the Phase IV CAQH CORE Operating Rule Set.

This rule supports the CAQH CORE Guiding Principles that CAQH CORE Operating Rules will not be based on the least common denominator but rather will encourage feasible progress, and that CAQH CORE Operating Rules are a floor and not a ceiling, i.e., entities can go beyond the Phase IV CAQH CORE Operating Rules.

3.7 Assumptions

A goal of this rule is to adhere to the principles of electronic data interchange (EDI) in assuring that transactions sent are accurately received and to facilitate correction of errors for electronically submitted premium payments.

The following assumptions apply to this rule:

- A successful communication connection has been established.
- This rule is a component of the larger set of Phase IV CAQH CORE Operating Rules; as such, all the CAQH CORE Guiding Principles apply to this rule and all other rules.
- This rule is not a comprehensive companion document addressing any content requirements of the ASC X12N v5010 820 or the ASC X12C v5010 999 transactions.
- Compliance with all CAQH CORE Operating Rules is a minimum requirement; any entity is free to offer more than what is required in the rule.

3.8 Abbreviations and Definitions Used in This Rule

Batch (Batch Mode, Batch Processing Mode)[49]**:** Batch Mode is when the initial (first) communications session is established and maintained open and active only for the time required to transfer a batch file of one or more transactions. A separate (second) communications session is later established and maintained open and active for the time required to acknowledge that the initial file was successfully received and/or to retrieve transaction responses.

Batch Mode/Batch Processing Mode is also considered to be an asynchronous processing mode, whereby the associated messages are chronologically and procedurally decoupled. In a request-response interaction, the client agent can process the response at some indeterminate point in the future when its existence is discovered. Mechanisms to implement this capability may include: polling, notification by receipt of another message, receipt of related responses (as when the request receiver "pushes" the corresponding responses back to the requestor), etc.

Batch Mode/Batch Processing Mode is from the perspective of both the request initiator and the request responder. If a Batch (asynchronous) request is sent via intermediaries, then such intermediaries may, or may not, use Batch Processing Mode to further process the request.

Processing Mode: Refers to when the payload of the connectivity message envelope is processed by the receiving system, i.e., in Real Time or in Batch mode.

Real Time (Real Time Mode, Real Time Processing Mode)[50]**:** Real Time Mode is when an entity is required to send a transaction and receive a related response within a single communications session, which is established

[49] Ibid.
[50] See Phase I CAQH CORE Glossary**:** http://www.caqh.org/sites/default/files/core/phase-i/reference/PIGlossary.pdf.

and maintained open and active until the required response is received by the entity initiating that session. Communication is complete when the session is closed.

Real Time Mode/Real Time Processing Mode is also considered to be a synchronous processing mode.

Real Time Mode/Real Time Processing Mode is from the perspective of both the request initiator and the request responder.

Safe Harbor: A "Safe Harbor" is generally defined as a statutory or regulatory provision that provides protection from a penalty or liability.[51]

In many IT-related initiatives, a safe harbor describes a set of standards/guidelines that allow for an "adequate" level of assurance when business partners are transacting business electronically.

The CAQH CORE Connectivity Safe Harbor requires the implementation of the Phase IV CAQH CORE 470 Connectivity Rule v4.0.0 so that application vendors, providers, and health plans (or other information sources) can be assured the CAQH CORE Connectivity Rule will be supported by any trading partner. All entities must demonstrate the ability to implement connectivity as described in Phase IV CAQH CORE 470 Connectivity Rule v4.0.0.

4 Rule Requirements

4.1 Payroll Deducted and Other Group Premium Payment for Insurance Products Processing Mode Requirements

A HIPAA-covered health plan or its agent must implement the server requirements for Batch Processing Mode for the ASC X12N v5010 820 transaction as specified in the Phase IV CAQH CORE 470 Connectivity Rule v4.0.0. Optionally, a HIPAA-covered health plan or its agent may elect to also implement the server requirements for Real Time Processing Modes for the ASC X12N v5010 820 transaction as specified in the Phase IV CAQH CORE 470 Connectivity Rule v4.0.0.

A HIPAA-covered health plan or its agent may also elect to implement the client requirements as specified in the Phase IV CAQH CORE 470 Connectivity Rule v4.0.0 in addition to implementing the server requirements. When a HIPAA-covered health plan or its agent elects to implement the client requirements as specified in the Phase IV CAQH CORE 470 Connectivity Rule v4.0.0 it must comply with all requirements specified in Sections 4.2, 4.3, 4.4, 4.5, 4.6, 5 and all respective Subsections.

The Phase IV CAQH CORE 470 Connectivity Rule v4.0.0 Real Time Processing Mode requirements are applicable when Real Time Processing Mode is offered for these transactions. The Phase IV CAQH CORE 470 Connectivity Rule v4.0.0 Batch Processing Mode requirements are applicable when Batch Processing Mode is offered for these transactions.

A HIPAA-covered health plan or its agent conducting the ASC X12N v5010 820 transaction is required to conform to the processing mode requirements specified in this section regardless of any other connectivity modes and methods used between trading partners.

[51] Merriam-Webster's Dictionary of Law. Merriam-Webster, Inc., 28 May, 2007. <Dictionary.com http://dictionary.reference.com/browse/safeharbor>

4.2 Payroll Deducted and Other Group Premium Payment for Insurance Products Connectivity Requirements

A HIPAA-covered entity or its agent must be able to support the Phase IV CAQH CORE 470 Connectivity Rule v4.0.0.

This connectivity rule addresses usage patterns for Real Time and Batch Processing Modes, the exchange of security identifiers, and communications-level errors and acknowledgements. It does not attempt to define the specific content of the message payload exchanges beyond declaring the formats that must be used between entities and that security information must be sent outside of the message envelope payload.

All HIPAA-covered entities must demonstrate the ability to implement connectivity as described in Phase IV CAQH CORE 470 Connectivity Rule v4.0.0. The Phase IV CAQH CORE 470 Connectivity Rule v4.0.0 is designed to provide a "Safe Harbor" that application vendors, providers and health plans or other entities can be assured will be supported by any trading partner. Supported means that the entity is capable and ready at the time of the request by a trading partner to exchange data using the Phase IV CAQH CORE 470 Connectivity Rule v4.0.0. These requirements are not intended to require trading partners to remove existing connections that do not match the rule, nor are they intended to require that all trading partners must use this method for all new connections. CAQH CORE expects that in some technical circumstances, trading partners may agree to use different communication mechanism(s) and/or security requirements than those described by these requirements.

4.3 Payroll Deducted and Other Group Premium Payment for Insurance Products System Availability

Many health plan issuers and their trading partners have a need to conduct premium payment transactions outside of the typical business day and business hours. Additionally, many health plan issuers and their trading partners are now allocating staff resources to performing administrative and financial back-office activities on weekends and evenings. As a result, health plan issuers and their trading partners have a business need to be able to conduct premium payment transactions at any time.

On the other hand, health plan issuers and their trading partners have a business need to periodically take their premium payment processing and other systems offline in order to perform required system maintenance. This typically results in some systems not being available for timely processing of ASC X12N v5010 820 transaction and ASC X12C v5010 999 transaction on certain nights and weekends. This rule requirement addresses these conflicting needs.

4.3.1 System Availability Requirements

System availability must be no less than 86 percent per calendar week for both Real Time and Batch Processing Modes. System is defined as all necessary components required to process an ASC X12N v5010 820 transaction and an ASC X12C v5010 999 transaction. Calendar week is defined as 12:01 a.m. Sunday to 12:00 a.m. the following Sunday. This will allow for a HIPAA-covered health plan or its agent to schedule system updates to take place within a *maximum* of 24 hours per calendar week for regularly scheduled downtime.

4.3.2 Reporting Requirements

4.3.2.1 Scheduled Downtime

A HIPAA-covered health plan or its agent must publish its regularly scheduled system downtime in an appropriate manner (e.g., on websites or in Companion Guides) such that the HIPAA-covered health plan's trading partners can determine the health plan's system availability so that staffing levels can be effectively managed.

4.3.2.2 Non-Routine Downtime

For non-routine downtime (e.g., system upgrade), a HIPAA-covered health plan or its agent must publish the schedule of non-routine downtime at least one week in advance.

4.3.2.3 Unscheduled Downtime

For unscheduled/emergency downtime (e.g., system crash), a HIPAA-covered health plan or its agent are required to provide information within one hour of realizing downtime will be needed.

4.3.2.4 No Response Required

No response is required during scheduled, non-routine, or unscheduled downtime(s).

4.3.2.5 Holiday Schedule

Each HIPAA-covered health plan or its agent will establish its own holiday schedule and publish it in accordance with the rule requirements above.

4.4 Payroll Deducted and Other Group Premium Payment for Insurance Products Real Time Processing Mode Response Time Requirements

Maximum response time for the receipt of an ASC X12C v5010 999 transaction from the time of submission of an ASC X12N v5010 820 must be 20 seconds when processing in Real Time Processing Mode.

Each HIPAA-covered entity or its agent must support this *maximum* response time requirement to ensure that at least 90 percent of all required responses are returned within the specified maximum response time as measured within a calendar month.

Each HIPAA-covered entity or its agent must capture, log, audit, match, and report the date (YYYYMMDD), time (HHMMSS) and control numbers from its own internal systems and the corresponding data received from its trading partners.

The recommended maximum response time between each participant in the transaction routing path is 4 seconds or less per hop as long as the 20-second total roundtrip *maximum* requirement is met.

Each HIPAA-covered entity or its agent must support these response time requirements in this section and other CAQH CORE Operating Rules regardless of the connectivity mode and methods used between trading partners.

The goal of this requirement is to adhere to the principles of EDI in assuring that transactions sent are accurately received and to facilitate correction of errors in Functional Groups of ASC X12N v5010 820 transaction.

This requirement assumes a successful communication connection has been established.

4.5 Payroll Deducted and Other Group Premium Payment for Insurance Products Real Time Processing Mode Acknowledgement Requirements

A HIPAA-covered health plan or its agent must return an ASC X12C v5010 999 transaction to indicate that a Functional Group(s) or Transaction Set(s) is accepted, accepted with errors, or rejected and must report each error detected to the most specific level of detail supported by the ASC X12C v5010 999 transaction.

4.6 Payroll Deducted and Other Group Premium Payment for Insurance Products Batch Processing Mode Response Time Requirements

Maximum response time for availability of ASC X12C v5010 999 transaction when processing an ASC X12N v5010 820 transaction submitted in Batch Processing Mode by 9:00 pm Eastern Time of a business day by a health plan sponsor or its agent must be no later than 7:00 am Eastern Time the third business day following submission.

A business day consists of the 24 hours commencing with 12:00 am (Midnight or 0000 hours) of each designated day through 11:59 pm (2359 hours) of that same designated day. The actual calendar day(s) constituting business days are defined by and at the discretion of each HIPAA-covered health plan or its agent.

Each HIPAA-covered entity or its agent must support this *maximum* response time requirement to ensure that at least 90 percent of all required responses are returned within the specified maximum response time as measured within a calendar month.

Each HIPAA-covered entity or its agent must capture, log, audit, match, and report the date (YYYYMMDD), time (HHMMSS) and control numbers from its own internal systems and the corresponding data received from its trading partners.

Each HIPAA-covered entity or its agent must support these response time requirements in this section and other CAQH CORE Operating Rules regardless of the connectivity mode and methods used between trading partners.

The goal of this requirement is to adhere to the principles of EDI in assuring that transactions sent are accurately received and to facilitate correction of errors in Functional Groups of ASC X12N v5010 820 transactions.

This requirement assumes a successful communication connection has been established.

4.7 Payroll Deducted and Other Group Premium Payment for Insurance Products Batch Processing Mode Acknowledgement Requirements

A HIPAA-covered health plan or its agent must return an ASC X12C v5010 999 transaction for each Functional Group of ASC X12N v5010 820 transactions:

- To indicate that the Functional Group(s) was either accepted, accepted with errors, or rejected

And

- To specify for each included ASC X12N v5010 820 transaction that the transaction set was either accepted, accepted with errors, or rejected.

The HIPAA-covered health plan or its agent must not return the ASC X12C v5010 999 transaction during the initial communications session in which the ASC X12N v5010 820 transaction is submitted.

When a Functional Group of ASC X12N v5010 820 of transactions is either accepted with errors or rejected, the ASC X12C v5010 999 transaction must report each error detected to the most specific level of detail supported by the ASC X12C v5010 999 transaction.

4.8 Elapsed Time for Internal Application System Processing of Received Premium Payment Data

A HIPAA-covered health plan or its agent must process the Payroll Deducted and Other Group Premium Payment for Insurance Products data by its internal application system within five business days following the successful receipt and validation of the data. In the context of this rule

- *Successful Receipt* means that the ASC X12N v5010 820 transaction has not been rejected by the health plan or its agent's EDI management system

And

- *Validation* means that any data inconsistencies detected in an accepted ASC X12N v5010 820 transaction which would prevent accurate posting of that data to the health plan or its agent's internal application system have been resolved.

4.9 Payroll Deducted and Other Group Premium Payment for Insurance Products Companion Guide

A HIPAA-covered health plan or its agent has the option of creating a "Companion Guide" that describes the specifics of how it will implement the HIPAA transactions. The Companion Guide is in addition to and supplements the ASC X12 TR3 Implementation Guide adopted for use under HIPAA.

Currently HIPAA-covered health plans or their agents have independently created Companion Guides that vary in format and structure. Such variance can be confusing to trading partners who must review numerous Companion Guides along with the ASC X12 TR3 Implementation Guides. To address this issue, CAQH CORE developed the CAQH CORE v5010 Master Companion Guide Template for health plans or their agents. Using this template, health plans or their agents can ensure that the structure of their Companion Guide is similar to other health plan's documents, making it easier for its trading partners to find information quickly as they consult each health plan's document on these important industry EDI transactions.

Developed with input from multiple health plans, system vendors, provider representatives, and health care/HIPAA industry experts, this template organizes information into several simple sections – General Information (Sections 1-9) and Transaction-Specific Information (Section 10) – accompanied by an appendix. Note that the Companion Guide template is presented in the form of an example from the viewpoint of a fictitious Acme Health Plan.

Although CAQH CORE believes that a standard template/common structure is desirable, it recognizes that different health plans may have different requirements. The CAQH CORE v5010 Master Companion Guide template gives health plans the flexibility to tailor the document to meet their particular needs.

4.9.1 Payroll Deducted and Other Group Premium Payment for Insurance Products Companion Guide Requirements

If a HIPAA-covered entity or its agent publishes a Companion Guide covering the ASC X12N v5010 820 transaction, the Companion Guide must follow the format/flow as defined in the CAQH CORE v5010 Master Companion Guide Template for HIPAA Transactions (CAQH CORE v5010 Master Companion Guide Template available HERE).

NOTE: This rule does not require any entity to modify any other existing Companion Guides that cover other HIPAA-mandated transaction implementation guides.

5 Conformance Requirements

Conformance with this CAQH CORE Operating Rule can be voluntarily demonstrated and certified through successful completion of the Phase IV CAQH CORE Voluntary Certification Test Suite with a third party CAQH CORE-authorized Testing Vendor, followed by the entity's successful application for a CORE Certification Seal. A CORE Certification Seal demonstrates that an entity has successfully tested for conformity with all of the Phase IV CAQH CORE Operating Rules, and the entity or its product has fulfilled all relevant conformance requirements.

Only the Department of Health and Human Services (HHS) can decide whether a particular HIPAA-covered entity's system is **compliant** or **noncompliant** with the HIPAA Administrative Simplification requirements (which include HIPAA-adopted CAQH CORE Operating Rules). HHS may adjudicate on a HIPAA-covered entity's compliance and assess civil money penalties or penalty fees for noncompliance under the following HIPAA Administrative Simplification mandates:

- HIPAA regulations mandate that the Secretary "will impose a civil money penalty upon a covered entity or business associate if the Secretary determines that the covered entity or business associate has violated an administrative simplification provision." (47 CFR 160.402)
- Under the ACA, HIPAA mandates a certification process for HIPAA-covered health plans only, under which HIPAA-covered health plans are required to file a statement with HHS certifying that their data and information systems are in compliance with applicable standards and associated operating rules. (Social Security Act, Title XI, Section 1173(h)) HIPAA also mandates that a HIPAA-covered health plan must "ensure that any entities that provide services pursuant to a contact with such health plan shall comply with any applicable certification and compliance requirements." (Social Security Act, Title XI, Section 1173(h)(3))
- Under the ACA, HIPAA also mandates that HHS is to "conduct periodic audits to ensure that health plans…are in compliance with any standards and operating rules." (Social Security Act, Title XI, Section 1173(h))

6 Appendix

6.1 Appendix 1: Reference

- ASC X12C 005010X231 Implementation Acknowledgement for Health Care Insurance (999) Technical Report Type 3 and associated errata
- ASC X12N 005010X218 Payroll Deducted and Other Group Premium Payment for Insurance Products (820) Technical Report Type 3 Implementation Guide and associated errata

Phase IV CAQH CORE 470 Connectivity Rule v4.0.0

September 2015

Table of Contents

1 Background

Each Phase of CAQH CORE Operating Rules builds on the previous phases to encourage feasible industry progress. Continuing to build on the Phase I, II, and III CAQH CORE Operating Rules, the Affordable Care Act (ACA) Section 1104 has mandated that CAQH CORE Operating Rules should be adopted that include rules around the health care claims and encounter reporting, health care services request for review and response, health plan premium payment, benefit enrollment and maintenance transactions, and attachments to allow the industry to leverage its investment in the Phase I, II, and III CAQH CORE Rules and apply them to exchanging the following HIPAA mandated transactions:

- ASC X12N 005010X223 Health Care Claim Institutional (837) ASC X12N 005010X222 Health Care Claim Professional (837) and ASC X12N 005010X224 Health Care Claim Dental (837) and their respective errata (collectively hereafter referenced as ASC X12N 837 v5010 Claim)
- ASC X12N 005010X217 Health Care Services Review – Request for Review and Response (278) and associated errata (hereafter referenced as ASC X12N v5010 278 Request and Response and referred to as prior authorization in general)
- ASC X12N 005010X218 Payroll Deducted and Other Group Premium Payment for Insurance Products (820) and associated errata (hereafter referenced as ASC X12N v5010 820)
- ASC X12N 005010X220 Benefit Enrollment and Maintenance (834) and associated errata (hereafter referenced as ASC X12N v5010 834)

The use of the ASC X12N v5010 820 and ASC X12N v5010 834 transactions by the Insurance Exchanges[52] is out of scope for this Phase IV CAQH CORE 470 Connectivity Rule v4.0.0.

Note: HHS has not adopted a standard for health claims attachments or indicated what standard(s) it might consider for the transaction, and an effective date for these operating rules is not included in the ACA. Thus, the immediate focus of this Phase IV CAQH CORE 470 Connectivity Rule v4.0.0 will not include attachments.

The Phase IV CAQH CORE 470 Connectivity Rule v4.0.0 was developed using a consensus-based approach among industry stakeholders, and is designed to facilitate interoperability, improve utilization of administrative transactions, enhance efficiency and lower the cost of information exchange in healthcare. Therefore, a key goal of this Phase IV CAQH CORE 470 Connectivity Operating Rule v4.0.0 is to continue to facilitate the industry's momentum to increase access to the HIPAA-mandated administrative transactions and to enable all HIPAA-covered entities or their agents[53], business associates, intermediaries, and vendors to build on and extend the connectivity and infrastructure capabilities established for the eligibility and claim status transactions in Phase I and II of CAQH CORE Operating Rules, which were then applied to the electronic remittance advice transaction in Phase III of CAQH CORE operating rules.

An important component of this goal is to further facilitate interoperability by moving the healthcare industry to a single message envelope[54] standard along with a single submitter authentication[55] method as set forth in Section 2.2.2 of the ACA-mandated Phase II CAQH CORE Connectivity 270 Rule v2.2.0.

---

[52] 45 CFR §155.20 Definitions. *Exchange* means a governmental agency or non-profit entity that meets the applicable standards of this part and makes QHPs available to qualified individuals and/or qualified employers. Unless otherwise identified, this term includes an Exchange serving the individual market for qualified individuals and a SHOP serving the small group market for qualified employers, regardless of whether the Exchange is established and operated by a State (including a regional Exchange or subsidiary Exchange) or by HHS.

[53] One who agrees and is authorized to act on behalf of another, a principal, to legally bind an individual in particular business transactions with third parties pursuant to an agency relationship. Source: West's Encyclopedia of American Law, edition 2. Copyright 2008 The Gale Group, Inc. All rights reserved.

[54] See §7.2 Abbreviations and Definitions Used in this Rule.

[55] Ibid.

An ancillary goal of this Phase IV CAQH CORE 470 Connectivity Rule v4.0.0 is to reinforce and clarify the "safe harbor"[56] established in Phase I CAQH CORE 153 Connectivity Rule and Phase II CAQH CORE 270 Connectivity Rule that application vendors, providers and health plans, business associates or other intermediaries can be assured will be supported by any HIPAA-covered entity or its agent. Essentially, all HIPAA-covered entities or their agents must support the connectivity requirements as specified in this rule. Clarification of the "safe harbor" addresses the requirement that when a HIPAA-covered entity or its agent are exchanging the transactions addressed by this rule using any other connectivity method as permitted by the CAQH CORE Safe Harbor, the Processing Mode requirements specified in the Phase IV CAQH CORE-required Processing Mode Table also apply. (See §5.) However, this rule is not intended to require trading partners to remove existing connections that do not match the rule, nor is it intended to require that all trading partners must use this method for all new connections. CAQH CORE expects that in some technical circumstances, trading partners may agree to use different communication mechanism(s) and/or security requirements than that described by this rule.

1.1 Affordable Care Act Mandates

This CAQH CORE Rule is part of a set of rules that addresses requirements in Section 1104 of the Affordable Care Act (ACA). Section 1104 contains an industry mandate for the use of operating rules to support implementation of the HIPAA standards. Using successful, yet voluntary, national industry efforts as a guide, Section 1104 defines operating rules as "the necessary business rules and guidelines for the electronic exchange of information that are not defined by a standard or its implementation specifications." As such, operating rules build upon existing healthcare transaction standards. The ACA outlines three sets of healthcare industry operating rules to be approved by the Department of Health and Human Services (HHS) and then implemented by the industry.

The third set of ACA-mandated operating rules address the health care claims or equivalent encounter information transactions, enrollment and disenrollment in a health plan, health plan premium payments, claims attachments, and referral certification and authorization.[57] The ACA requires HHS to adopt a set of operating rules for these five transactions by July 2014[58]. In a letter dated 09/12/12 to the Chairperson of the National Committee on Vital and Health Statistics (NCVHS),[59] the Secretary of HHS designated CAQH CORE as the operating rule authoring entity for the remaining five HIPAA-mandated electronic transactions.

Section 1104 of the ACA also adds the health claims attachment transaction to the list of electronic healthcare transactions for which the HHS Secretary must adopt a standard under HIPAA. The ACA requires the health claims attachment transaction standard to be adopted by 01/01/14, in a manner ensuring that it is effective by 01/01/16.[60]

1.2 Industry Neutral Standards Addressed in this Rule

This Phase IV CAQH CORE 470 Connectivity Rule v4.0.0 addresses industry neutral transport, transport security, message envelope, and submitter authentication standards as well as CAQH CORE specified message envelope metadata,[61, 62] for both Real Time and Batch Processing Modes of transmitted transactions, and communications-level errors and acknowledgements. These standards include the public Internet, Hypertext Transport Protocol (HTTP), Secure Sockets Layer (SSL), Transport Layer Security (TLS), SOAP, MTOM, XSD, WSDL, and the X.509 Digital Certificate for submitter authentication.

---

[56] See §5 Safe Harbor and §7.2 Abbreviations and Definitions Used in this Rule.
[57] The first set of operating rules under ACA Section 1104 applies to eligibility and claim status transactions; these operating rules were effective 01/01/13. The second set of operating rules applies to EFT and ERA; these operating rules were effective 01/01/14.
[58] This date is statutory language and statutory language can be changed only by Congress.
[59] 09/12/12 HHS Letter from the Secretary to the Chairperson of NCVHS.
[60] This date is statutory language and statutory language can be changed only by Congress.
[61] See §7.2 Abbreviations and Definitions Used in this Rule.
[62] See §4.4 Envelope Metadata Fields, Descriptions, Intended Use and Syntax/Value Sets and §7.2 Abbreviations and Definitions Used in this Rule.

2 Issues to be Addressed and Business Justification

2.1 Problem Space

Recognizing that the healthcare industry uses multiple connectivity methods for electronic administrative transactions – some based on open standards, others on proprietary approaches – in Phases I, II and III the CAQH Committee on Operating Rules for Information Exchange (CORE®) aimed to fill that gap by formulating connectivity and security rules to support healthcare industry specific transactions. Requirements related to connectivity, infrastructure, e.g., response times, companion guides, system availability, etc., were addressed in multiple transaction-specific operating rules. The Phase I and Phase II CAQH CORE Connectivity Operating Rules specifically addressed the message envelope, corresponding envelope metadata, vocabularies and semantics needed, Real Time and Batch Processing Modes, and the industry's developing use of the public Internet. However, there were challenges experienced by the industry when implementing the Phase I and Phase II CAQH CORE Connectivity Operating Rules, which this Phase IV CAQH CORE 470 Connectivity Rule v4.0.0 addresses, e.g.:

- Complexity: Provides a simpler and more prescriptive rule with fewer options (e.g., single envelope standard, and single authentication standard)
- Transaction Support: Provides more robust and uniform support for handling transaction payload by requiring MTOM for SOAP (both Real Time and Batch Processing Mode); provides better support for the new set of transactions relative to the previous rules, e.g., by supporting additional message interactions
- Security: Improves security by removing Username+Password which is a weak form of B2B authentication, and by requiring the use of only X.509 Client Certificate-based authentication over SSL/TLS, which is a stronger form of authentication. Improves support for FIPS 140-2 compliance for entities requiring such compliance, in terms of transport security and message envelope security

2.2 CAQH CORE Process in Addressing the Problem Space

As part of the development of the Phase IV CAQH CORE 470 Connectivity Rule v4.0.0 environmental scans as well as extensive business and market analysis were conducted to gain insights into the current industry landscape regarding legislative, market movements and national initiatives. The results of these efforts identified several potential opportunity areas as a focus for the Phase IV CAQH CORE 470 Connectivity Operating Rule v4.0.0. Table 2.2-1 below summarizes at a high level the potential opportunity areas identified.

Table 2.2-1 Potential Phase IV CAQH CORE Connectivity Rule Opportunities
Opportunity Area A: Improving Rule Language/Clarity
Rule Opportunity #1: Improve clarity around Real Time and Batch requirements, error handling
Rule Opportunity #2: Address CAQH CORE Connectivity Rule v2.2.0 implementer feedback specific to technical issues
Opportunity Area B: Enhancing Envelope Standards and Metadata
Rule Opportunity #3: Expand ongoing payload-agnostic approach for explicitly enumerating Payload Types for transactions newly mandated by ACA
Rule Opportunity #4: Explore convergence of Envelope Standards
Rule Opportunity #4A: Explore Suitability of other envelope approaches (e.g., JavaScript Object Notation (JSON))
Opportunity Area C: Enhancing Reliability and Security
Rule Opportunity #5: Reliable and secure handling of attachments
Rule Opportunity #6: Explore convergence of Authentication Standards
Rule Opportunity #7: Explore industry-wide policy for uniform use of digital certificates
Rule Opportunity #8: Explore TLS 1.X as part of base requirement for transport security
Rule Opportunity #9: Explore enhanced envelope level security (e.g., Signature, SAML Authorization),

Table 2.2-1 Potential Phase IV CAQH CORE Connectivity Rule Opportunities
determining B2B nature of transactions and that some signatures may be applied at the document (payload) level.
Opportunity Area D: Exploring Additional Transport Options
Rule Opportunity #10: Explore support for ONC DIRECT as an additional transport option
Rule Opportunity #11: Explore support for Representational State Transfer (REST) as an additional transport option
Rule Opportunity #12: Explore support for Secure File Transfer Protocol (SFTP) as an additional transport option
Opportunity Area E: Specificity Around Message Interaction Requirements
Rule Opportunity #13: Defining Transaction Specific Message Interaction (e.g., Real Time, Batch) Requirements

To select the opportunities that would provide the best value to the industry CAQH CORE developed an objective approach using a set of 44 business and technical criteria to evaluate and compare the potential rule opportunities identified for Phase IV CAQH CORE Connectivity, recognizing that all of the CAQH CORE Rules are expected to evolve in future phases. Some key business and technical criteria among them are that the Phase IV CAQH CORE 470 Connectivity Rule v4.0.0 will:

- Not create or promote proprietary approaches to electronic interactions/transactions
- Not be based on the least common denominator but rather will encourage feasible progress, promote cost savings, and efficiency
- Address both Batch and Real Time Processing Modes, with a movement towards Real Time (where/when appropriate)
- Be developed using a consensus-based, multi-stakeholder approach
- Builds upon existing standards
- Be focused on Business to Business (B2B) transactions
- Create a base and not a "ceiling"
- Be vendor neutral
- Be built upon HIPAA, and align with other key industry bodies in order to promote interoperability
- Address interest in XML, or other evolving standards where appropriate
- Support the Guiding Principles of HHS' Nationwide Health Information Network (now the eHealth Information Exchange[63])

Table 2.2-2 shows the results of applying the business and technical criteria to the potential rule opportunities.

Table 2.2-1 Rule Opportunity Selection		
Rule Opportunities To Be Addressed In Phase IV	**Rule Opportunities To Be Addressed In Phase IV If Time Allows**	**Rule Opportunities Deferred For Future Consideration**
Rule Opportunity #1: Improve clarity around Real Time and Batch requirements, error handling	Rule Opportunity #5: Reliable and secure handling of attachments	Rule Opportunity #4A: Explore suitability of other envelope approaches (e.g., JavaScript Object Notation (JSON))
Rule Opportunity #2: Address CAQH CORE Connectivity Rule v2.2.0 implementer feedback specific to technical issues	Rule Opportunity #7: Explore industry-wide policy for uniform use of digital certificates	Rule Opportunity #11: Explore support for Representational State Transfer (REST) as an additional transport option

[63] See §7.2 Abbreviations and Definitions Used in this Rule

Table 2.2-1 Rule Opportunity Selection		
Rule Opportunities To Be Addressed In Phase IV	**Rule Opportunities To Be Addressed In Phase IV If Time Allows**	**Rule Opportunities Deferred For Future Consideration**
Rule Opportunity #3: Expand ongoing payload-agnostic approach for explicitly enumerating Payload Types for transactions newly mandated by ACA	Rule Opportunity #9: Explore enhanced envelope level security (e.g., Signature, SAML Authorization), determining B2B nature of transactions and that some signatures may be applied at the document (payload) level.	Rule Opportunity #12: Explore support for Secure File Transfer Protocol (SFTP) as an additional transport option
Rule Opportunity #4: Explore convergence of Envelope Standards	Rule Opportunity #10: Explore support for ONC DIRECT as an additional transport option	
Rule Opportunity #6: Explore convergence of Authentication Standards		
Rule Opportunity #8: Explore TLS 1.X as part of base requirement for transport security		
Rule Opportunity #13: Defining Transaction Specific Message Interaction (e.g., Real Time, Batch) Requirements		

2.3 Phase IV CAQH CORE 470 Connectivity Rule v4.0.0 Builds on Foundation Established by Previous CAQH CORE Connectivity Rules

2.3.1 Base Minimum Requirements Specified in the Phase I CAQH CORE 153 Connectivity Rule

The Phase I CAQH CORE 153 Connectivity Rule established the requirement to use the HTTP/S secure transport protocol over the public Internet. It also specified a minimum set of metadata that must be outside the ASC X12N payload (e.g., date/time, payload ID, and other elements), and aspects of connectivity/security such as connectivity response times, acknowledgements and errors. The Phase I CAQH CORE 153 Connectivity Rule also established the CAQH CORE Connectivity "Safe Harbor" which allows HIPAA-covered entities or their agents to implement other connectivity/security methods in addition to the requirement to support the CORE Connectivity Rule.

2.3.2 Phase II CAQH CORE 270 Connectivity Rule Specified Robust, Prescriptive Requirements

CAQH CORE was aware the Phase I CAQH CORE 153 Connectivity Rule did not provide the optimum level of specificity for implementations as it was developed as a first step. Voluntary CORE-certified implementations were based on many types of message enveloping methods: e.g., HTTP POST with name/value pairs, HTTP MIME Multipart, W3C XML Schema and SOAP+WSDL among others. Further, within each of these envelope method implementations, significant variations existed in field names and locations of Phase I CAQH CORE 153 Connectivity Rule metadata, message envelope structure, submitter authentication methods, routing approaches and security-related information. As a result, such variations among enveloping methods and metadata posed a major challenge for interoperability. Therefore, the Phase II CAQH CORE 270 Connectivity Rule specified more prescriptive requirements for message envelopes, message envelope metadata, and submitter authentication methods.

2.3.2.1 Two Message Envelope Standards Specified in Phase II CAQH CORE Rule

Just as paper documents need to be placed in an envelope (container), electronic documents (e.g., eligibility inquiries, electronic claims, etc.) must be placed into a container for electronic transmission from the sender to the receiver. These electronic containers, called message envelopes, must also include the critical information needed to identify the sender, receiver, and other information essential for ensuring the electronic documents in the message envelope are delivered to the intended recipient securely and reliably. For message envelopes the terms for the various pieces of information required are called Message Envelope Metadata specifying the fields and their corresponding values within the message envelope that describe the documents (message payload). A message envelope consists of a well-defined structure for organizing and formatting the message envelope metadata, which also includes other information, such as date, time, unique identifiers for each message envelope to enable reliable tracking and auditing.

The Phase II CAQH CORE 270 Connectivity Rule further facilitated interoperability by requiring the use of two message envelope standards that were shown to meet the agreed upon Phase II CAQH CORE Connectivity criteria, have significant installed base in the healthcare industry, and perform well under real world transaction loads. These two envelope standards were HTTP MIME Multipart and SOAP + WSDL.

Since both these standards have significant merits, the advantages and challenges of having a single envelope standard versus both of these envelope standards as part of the Phase II CAQH CORE 270 Connectivity Rule was debated. The major advantage of a rule based on a single envelope standard is that it would be more definitive and facilitate better interoperability. However, having just one standard would require implementers of the other envelope standard (i.e., the one that was not chosen) to modify their implementations to be compliant with the Phase II CAQH CORE 270 Connectivity Rule. Since both standards met the criteria and had large installed bases, CAQH CORE determined that convergence on a single standard in Phase II would create a barrier to adoption of the Phase II CAQH CORE 270 Connectivity Rule by a large segment of the industry.

2.3.2.2 Phase II CAQH CORE Rule Specified Two Submitter Authentication Methods

HIPAA Security regulations[64] at 45 CFR §164.304 Definitions define "authentication as the corroboration that a person [entity] is the one claimed" and further identifies that the "*Technical safeguards* are the technology and the policy and procedures for its use that protect electronic protected health information and control access to it." O'Reilly[65] goes on to further describe authentication as "The process of proving that a subject (e.g., a user or a system) is what the subject claims to be. Authentication is a measure used to verify the eligibility of a subject and the ability of that subject to access certain information. It protects against the fraudulent use of a system or the fraudulent transmission of information. There are three classic ways to authenticate oneself: something you know, something you have, and something you are."

Thus, it is essential to validate a particular entity's identity for granting access to sensitive data or functionalities contained within the system. One of the most common authentication methods used in general today is a Username+Password. Digital certificates are another commonly used method and are considered to "provide the most secure means of authenticating identities."[66] Each authentication method has advantages and disadvantages in terms of security, usability, and breadth of support. Password-based authentication methods, however, do not provide strong security.

Organizations that receive and process (or relay) requests (i.e., as a server) generally enforce a specific authentication method to control access to their resources. Supporting this authentication method is a credential issuance and management scheme defined by an organizational policy. The complexity of supporting two such policies and credential management mechanisms is high at the entity where submitter authentication is enforced

[64] 68 FR 8376, Feb. 20, 2003, as amended at 74 FR 42767, Aug. 24, 2009; 78 FR 5693, Jan. 25, 2013
[65] D. Russell and G.T. Gangemi Sr., "Computer Security Basics", O'Reilly & Associates, Inc., 1992
[66] Centers for Medicare & Medicaid Services, Enterprise Information Security Group, Risk Management Handbook volume III Standard 3.1, CMS Authentication Standards, Final Version 1.3, April 17, 20014

(server), but is relatively low at the submitter (client). For this reason, the Phase II CAQH CORE 270 Connectivity Rule required only server-side implementations to support one of two submitter authentication methods:

- Username+Password
- X.509 Digital Certificate

2.4 Phase IV CAQH CORE 470 Connectivity Rule v4.0.0 - Key Enhancements relative to Phase II CAQH CORE Connectivity Rule

To address the problems described in §2.1 and to advance the vision for future phases that was identified in Phase II and Phase III, this Phase IV CAQH CORE 470 Connectivity Rule v4.0.0 has key enhancements by converging on single envelope and authentication standard, improving transaction support for the third set of ACA-mandated transactions, and by improving robustness and security. These enhancements are described below.

2.4.1 Convergence on a Single Message Envelope Standard

The Phase II CAQH CORE 270 Connectivity Rule identified convergence to a single envelope standard as a vision for future phases of connectivity based on greater industry experience with implementing the two message envelope standards specified in the rule.

After extensive analysis CAQH CORE determined that converging on the use of SOAP+WSDL as the single message envelope standard in this Phase IV CAQH CORE 470 Connectivity Rule v4.0.0 includes these benefits:

- Limits variations in use of SOAP for real time and batch processing modes by requiring the use of MTOM for both processing modes
- Relatively simple rule change
- Significant ROI through improvements in interoperability
- Simplicity of rule requirements
- Reduction of implementation cost and complexity by having fewer options
- XML based and therefore extensible
- Good tooling support for SOAP in most platforms
- Alignment with clinical initiatives and industry trends

2.4.2 Convergence on a Single Submitter Authentication Method

The Phase II CAQH CORE 270 Connectivity Rule identified convergence to a single authentication standard as a vision for future phases of connectivity based on greater industry experience with implementing the two message authentication standards specified in the rule.

After extensive analysis CAQH CORE determined that converging on the use of the X.509 digital certificate as the single authentication standard in this Phase IV CAQH CORE 470 Connectivity Rule v4.0.0 includes these benefits:

- Relatively simple rule change
- Significant ROI through improvements in interoperability
- Simplicity of rule requirements
- Reduction of implementation cost and complexity by having fewer options
- X.509 client certificate-based authentication over SSL/TLS is significantly more secure than Username+Password
- Alignment with clinical initiatives and industry trends

2.4.3 Enhancements to Message Interactions

The Phase II CAQH CORE 270 Connectivity Rule defined message interactions for conducting Real Time and Batch interactions. Phase IV preserves the Real Time and Batch interactions while adding some message interactions that could be used as generic building blocks for supporting current or future transactions. The message interactions for the third set of ACA-mandated transactions are illustrated in Section 7 using Uniform Markup Language (UML) sequence diagrams, also known simply as sequence diagrams.

A sequence diagram is an interaction diagram used to visualize how a client (submitter) and a server (receiver) operate with one another and in what order for the transactions addressed by this Phase IV CAQH CORE 470 Connectivity Rule v4.0.0. Some interactions are scenarios in which the business transaction (message payload) is to be processed in Real Time by the server while other interactions are scenarios in which the business transaction(s) (message payload) are to be processed as a batch after the server has successfully received the batch and the communication session has ended. When an interaction includes multiple client requests and server responses, e.g., a batch of health care claims, each pair of interactions and its corresponding (synchronous) response is shown in the sequence diagram. The UML sequence diagrams in this Phase IV CAQH CORE 470 Connectivity Rule v4.0.0 are specific to the HIPAA mandated transactions to which this rule applies.

2.4.4 Improved Support for Security Compliance and Stronger Security

The Phase II CAQH CORE 270 Connectivity Rule v2.2.0 requires the implementation of the Secure Sockets Layer (SSL) v3.0 as a minimum while optionally allowing entities to implement the Transport Layer Security (TLS) v1.0 or higher when an entity is required to comply with the National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS 140).

Analysis conducted by CAQH CORE indicated that while SSL v3.0 is commonly used in the industry, some HIPAA-covered entities or their agents (e.g., Federal government trading partners, eHealth Exchange) are required to also comply with the FIPS 140-2, which essentially prohibits the use of SSL v3.0 and TLS v1.0. As per NIST 800-52r1, federal government entities are required to implement TLS 1.1 or higher. Relative to SSL v3.0, TLS 1.1 and to a larger extent, TLS 1.2 has improvements in security for data in transit (e.g., in message integrity, encryption algorithms, and key generation). However, platform and programming support for, and industry experience in implementing TLS 1.1 and TLS 1.2 is limited at this time. Considering this, this Phase IV CAQH CORE 470 Connectivity Rule v4.0.0 (See §3.2) strikes a balance between the need to accommodate HIPAA-covered entities or their agents that must also comply with FIPS 140-2, while allowing non-government entities to continue using non-FIPS compliant security at the transport security layer as well as at the message envelope security layer.

Further, by allowing the use of TLS 1.1 or higher in lieu of SSL v3.0 for both FIPS 140-2 compliance and for the sake of stronger security, this Phase IV CAQH CORE 470 Connectivity Rule v4.0.0 (See §3.2) enables a transition path from SSL v3.0 to TLS 1.1 or higher.

2.4.5 CAQH CORE Process for Maintaining Processing Mode & Payload Type Specifications

Processing modes or computing modes are classifications of different types of computer processing, e.g., Batch, Real Time.[67] In the context of CAQH CORE Operating Rules, the concept of processing mode applies to the timeframe within which a receiver of a payload of transactions processes those transactions and returns to the sender a payload of appropriate acknowledgements.

A message payload is the essential data that is being routed between a sender and a receiver during a connectivity session. In the context of this CAQH CORE Operating Rule, a payload could be one or more healthcare claims or referral requests, etc. In order to enable efficient and effective handling of the various kinds of payloads that could be exchanged, a unique "payload type identifier" is assigned to each kind of payload.

[67] See §7.2 Abbreviations and Definitions Used in this Rule.

As this rule becomes widely adopted and implemented in health care the experience and learning gained from implementers CAQH CORE recognizes there may be a need to modify either the Phase IV CAQH CORE Processing Mode requirements or the Phase IV CAQH CORE Payload Types or both in order to be agile and flexible in meeting emerging or new industry needs. To meet this anticipated need to enable review and maintenance of the processing modes for the administrative transactions addressed by this rule and payload type identifiers are specified in a separate companion document to this rule. A process and policy to address the review and maintenance will be developed by CAQH CORE. (See §3.7.3)

The Phase IV CAQH CORE-required Payload Types Table includes payload type values for all HIPAA mandated ASC X12N v5010 transactions, including those transactions that are addressed in the Phase I and II CAQH CORE Operating Rules for eligibility, claim status and the Phase III CAQH CORE Operating Rules for ERA. While HIPAA-covered entities or their agents are required to use this Phase IV CAQH CORE 470 Connectivity Rule v4.0.0 for the exchange of claims, prior authorization, benefit enrollment and maintenance, and health plan premium payment transactions, subject to the Safe Harbor provisions of the Phase IV CAQH CORE 470 Connectivity Rule v4.0.0 HIPAA-covered entities or their agents may also use this Phase IV CAQH CORE 470 Connectivity Rule v4.0.0 for the exchange of eligibility, claim status and ERA transactions in accordance with the Safe Harbor provision of the Phase II CAQH CORE 270 Connectivity Rule v2.2.0. However, this does not permit any HIPAA-covered entity or its agent to discontinue support for the exchange of the eligibility, claim status and ERA transactions as required in the Phase II CAQH CORE 270 Connectivity Rule v2.2.0. HIPAA-covered entities or their agents may also use this Phase IV CAQH CORE 470 Connectivity Rule v4.0.0 for the exchange of ASC X12N transactions not mandated by HIPAA.

2.4.6 Backward Compatibility with Phase I and II CAQH CORE Connectivity Rules

CAQH CORE thoroughly examined maintaining *backward compatibility* with the Phase I and Phase II CAQH CORE Connectivity Rules while also evolving the Phase IV CAQH CORE 470 Connectivity Rule v4.0.0, which is applicable to a different set of administrative transactions[68]. These ACA-mandated CAQH CORE Operating Rules currently remain in effect and cannot be modified by Phase IV CAQH CORE Operating Rules. In general, the concept of *backward compatibility* in relationship to technical specifications means that implementers of a newer version of a specification will be able to interact and interoperate with implementers of a previous version easily and without major modifications to either version.

In the context of this Phase IV CAQH CORE 470 Connectivity Rule v4.0.0 *backward compatibility* means that key requirements to support two message envelope standards and two submitter authentication methods specified in previous versions of CAQH CORE Connectivity Rules would become an impediment to realizing some of the Phase IV high priority rule opportunities agreed to by CAQH CORE. (See §2.2 Table 2.2-2.) Since this Phase IV CAQH CORE Connectivity Rule v4.0.0 is intended to be independent of the current ACA-mandated CAQH CORE Operating Rules and must stand alone on its own merits, implementers of those rules are not required to de-implement or otherwise discontinue support for any of those rules.

Further, as HIPAA-covered entities or their agents may also use this Phase IV CAQH CORE 470 Connectivity Rule v4.0.0 for the exchange of transactions addressed by previous phases (Phase I and II) in accordance with the Safe Harbor provision of the Phase II CAQH CORE 270 Connectivity Rule v2.2.0, the improvements made in this Phase IV CAQH CORE Connectivity Rule v4.0.0 can also benefit those transactions. However, this does not permit any HIPAA-covered entity or its agent to discontinue support for the exchange of transactions addressed in CORE Phase II and CORE Phase III as required in the Phase II CAQH CORE 270 Connectivity Rule v2.2.0.

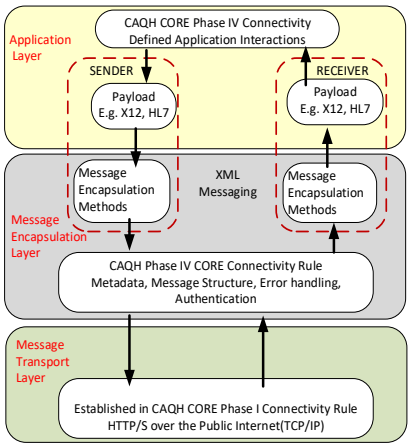
[68] The first set of operating rules under ACA Section 1104 applies to eligibility and claim status transactions; these operating rules were effective 01/01/13. The second set of operating rules applies to EFT and ERA; these operating rules were effective 01/01/14.

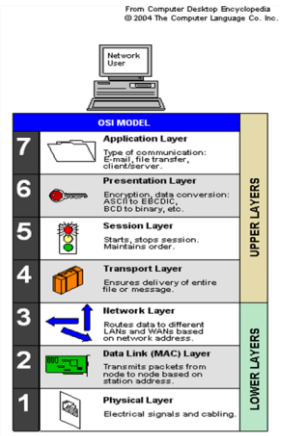
3 Scope

3.1 What the Rule Applies To

The technical scope of this Phase IV CAQH CORE Connectivity Rule v4.0.0 can be described in terms of the specific network layers within the Open Systems Interconnection Basic Reference Model[69] (OSI model). As shown in the diagram below, the scope of this Phase IV CAQH CORE Connectivity Rule v4.0.0 is OSI Layers 3 and 4 (Transport and Network layers) and OSI Layers 5 and 6 (Session and Presentation layers, also called Message Encapsulation layers).

Figure #3.1.1





OSI Model		Messaging Infrastructure Model
Application Layer	OSI 7	Application Layer
Presentation Layer	OSI 6	Message Encapsulation Layer (envelope)
Session Layer	OSI 5	
Transport Layer	OSI 4	Message Transport Layer
Network Layer	OSI 3	

Figure Notes:

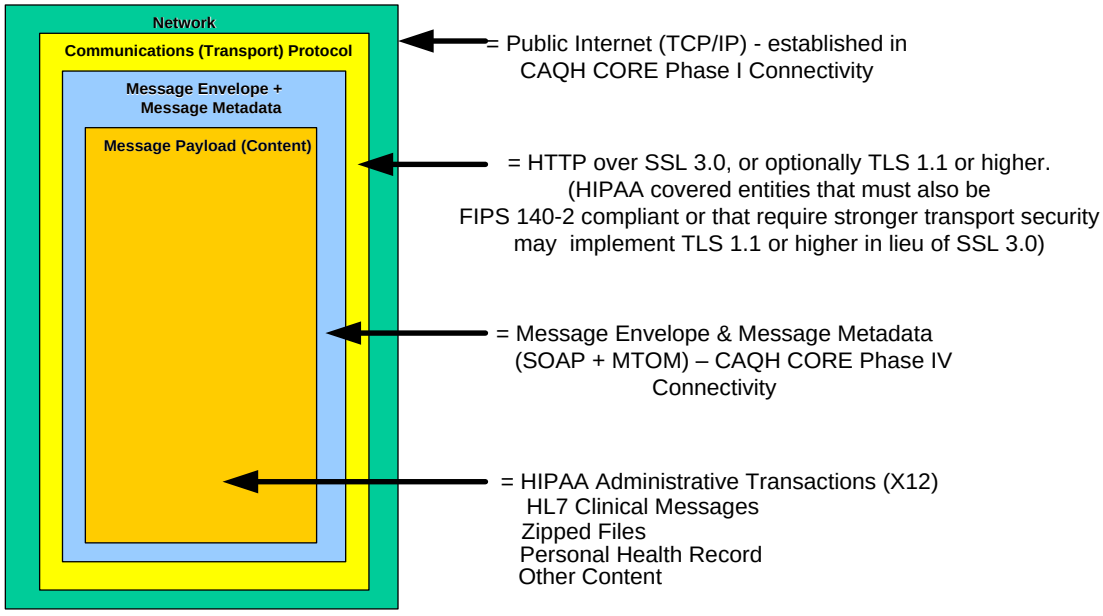
- CAQH CORE Phase IV Connectivity Rule addresses Layers 5 and 6 of the OSI Model
- Layer 3 and 4, the Transport Layer and Network Layer, was established as HTTP/S over the public internet in the CAQH CORE Phase I Connectivity Rule
- Layers 1 and 2 are not applicable to CORE because they are not items that could be included in a rule as these layers are so specific to the internal IT systems of every organization.

As shown in the Figure 3.1.1 above, typically an application file (or Payload) such as ASC X12 or HL7 is created or processed by an application that resides in the Application Layer (Layer 7 in the OSI Model). The Message Encapsulation layer (Layers 5 and 6 in the OSI Model) create a Message Envelope, and handles connectivity and security. The underlying layers (Layers 1 through 4) provide the necessary message transport and the network infrastructure (e.g., TCP/IP is provided at Layer 3).

As shown in Figure #3.1.2 below, the Message Envelope is outside the Message Payload (content), and inside the Transport Protocol envelope. Here, the Transport Protocol Envelope corresponds to OSI Model Layers 3 and 4, Message Envelope corresponds to OSI Model Layers 5 and 6, and Message Payload (content) corresponds to OSI Model Layer 7. The Phase I CAQH CORE 153 Connectivity Rule v1.1.0 established the CAQH CORE foundational use of HTTP/S as the transport protocol over the public Internet, hence the transport protocol envelope consists of HTTP headers. Examples of message payload include HIPAA administrative transactions (ASC X12N), HL7 clinical messages, zipped files, etc.

[69] Zimmerman, H., OSI Reference Model – ISO Model of Architecture for Open Systems Interconnection, IEEE Transactions on Communications, Vol. Com-28, No. 4, April 1980.

Figure #3.1.2



3.2 Standards Used in this Rule

The following is a list of standards and their versions on which this Rule is based:

- HTTP Version 1.1[70]
- SSL Version 3.0.
    - This does not preclude the optional use of TLS 1.1 (or a higher version) for connectivity with trading partners that require FIPS 140-2 compliance or whose security policies require the enhanced security afforded by TLS 1.1 or higher. Entities that must also be FIPS 140-2 compliant or whose security policies require enhanced security may implement TLS 1.1 or higher in lieu of SSL 3.0.
- SOAP Version 1.2
- WSDL Version 1.1

[70] Hereafter the combination of HTTP and SSL/TLS is referenced as HTTP/S.

3.3 When the Rule Applies

The Phase IV CAQH CORE 470 Connectivity Rule v4.0.0 applies when trading partners are exchanging any transaction specified in the third set of the Affordable Care Act (ACA) §1104 administrative transactions, i.e.:

- ASC X12N v5010 837 Claim
- ASC X12N v5010 278 Request and Response
- ASC X12N v5010 820
- ASC X12N v5010 834

The Phase IV CAQH CORE 470 Connectivity Rule v4.0.0 may also be applied to other payload types. Note: some entities may also apply this rule to other ASC X12N administrative transactions. This Phase IV CORE Connectivity Rule v4.0.0 is a Safe Harbor (See §5), and therefore only needs to be used if mutually agreed to by the trading partners. It is expected that in some instances, other or existing mechanisms may be more appropriate methods of connectivity. Further, HIPAA-covered entities or their agents may also use this Phase IV CAQH CORE 470 Connectivity Rule v4.0.0 for the exchange of eligibility, claim status and ERA transactions in accordance with the Safe Harbor provision of the Phase II CAQH CORE 270 Connectivity Rule v2.2.0. However, this does not permit any HIPAA-covered entity or its agent to discontinue support for the exchange of transactions addressed in CAQH CORE Phase II and CAQH CORE Phase III as required in the Phase II CAQH CORE 270 Connectivity Rule v2.2.0.

3.4 When the Rule Does Not Apply

The Phase IV CAQH CORE Connectivity Rule v4.0.0 **DOES NOT** apply in the following scenarios:

- When HIPAA-covered entities or their agents exchange payloads other than
    - ASC X12N v5010 837 Claim
    - ASC X12N v5010 278 Request and Response
    - ASC X12N v5010 820
    - ASC X12N v5010 834

This rule does not address requirements for the use of the ASC X12N v5010 820 and the ASC X12N v5010 834 transactions by the ACA Federal or state Health Information Exchanges (HIX).

This rule is designed to be payload agnostic, and as such it is expected that HIPAA-covered entities or their agents will use this methodology for other payloads as described in §3.3; however, the rule does not require this.

3.5 What the Rule Does Not Require

The Phase IV CAQH CORE Connectivity Rule v4.0.0 (See §5):

- **DOES NOT** require trading partners to discontinue existing connections that do not match the rule.
- **DOES NOT** require that trading partners must use a CAQH CORE-compliant method for all new connections.
- **DOES NOT** require that all CAQH CORE trading partners use only one method for all connections.
- **DOES NOT** require any HIPAA-covered entity or its agent to do business with any trading partner or other HIPAA-covered entity or its agent.

Further, the Phase IV CAQH CORE Connectivity Rule v4.0.0 **DOES NOT** require the following:

- Additional centralized services other than those that are already provided in the Internet (e.g., Domain name and TCP/IP routing services).

- Additional directories or data repositories.
- Additional centralized Public Key Infrastructure (PKI) Certificate Authorities, identity management or authentication servers.
- Use of specific hardware platforms, software or programming languages.

3.6 Outside the Scope of this Rule

The following items are outside the scope of this rule:

- The use of the message envelope and metadata defined in this rule for those messages that are sent over TCP/IP connections that are private (e.g., Intranet, leased lines, or VPN).
- Non-TCP/IP protocols such as packet switching (e.g., X.25, SNA, and Frame Relay).
- Submitter Authorization is a local decision at the site that receives a request.
- The list of trusted Certificate Authorities is a decision between trading partners.
- The maximum size of a batch file that is accepted by a Server. The Server implementer may publish its file size limit, if any, in its Connectivity Companion Guide. (See §4.2.6.2)

3.7 CAQH CORE-required Processing Mode and Payload Type Tables

This Phase IV CAQH CORE Connectivity Rule v4.0.0 is comprised of the complete rule itself, which specifies all rule requirements; and a companion document to the rule, which specifies additional rule requirements addressing Phase IV CAQH CORE-required Processing Modes and Payload Type Tables. This enables the necessary flexibility to review and maintain the processing modes and payload types based on Federal regulation or Federal notices to the industry impacting the transactions addressed by this rule.

3.7.1 CAQH CORE-required Processing Mode Table

The Phase IV CAQH CORE-required Processing Mode Table (see §4.4.3) specifies the comprehensive and normative processing mode requirements (i.e., Real Time and/or Batch) for the transactions addressed by this rule.

3.7.2 CAQH CORE-required Payload Type Table

The Phase IV CAQH CORE-required Payload Type Table (see §4.4.3) specifies the comprehensive and normative identifiers for the CORE Envelope Metadata Payload Type Element as defined in the Table of CORE Envelope Metadata. (See §4.4.2.)

The Payload Type identifiers specified in the Phase IV CAQH CORE-required Payload Type Table apply when an entity is exchanging the transactions addressed by this rule in conformance with the requirements specified in §4 and subsections.

3.7.3 Maintenance of the CAQH CORE-required Processing Mode and Payload Type Tables

CAQH CORE recognizes that as this rule becomes widely adopted and implemented in health care the experience and learning gained from implementers may indicate a need to modify either the Phase IV CAQH CORE-required Processing Mode Table or the Phase IV CAQH CORE-required Payload Type Table or both to meet emerging or new industry needs. Given this anticipated need a process and policy to enable the review and maintenance of these tables specified in the companion document to this rule, *COREProcessingModePayloadTypeTables.docx,* will be developed by CAQH CORE.

Such review and maintenance of either the Phase IV CAQH CORE-required Processing Mode Table or the Phase IV CAQH CORE-required Payload Type Table or both will follow standard CAQH CORE processes for rule revisions. CAQH CORE will develop such a process and policy for the first review of potential revisions of these tables in accordance with CAQH CORE Guiding Principles following the approval of the Phase IV CAQH CORE Operating Rules. The first review may commence

- One year after the passage of a Federal regulation requiring implementation of this CAQH CORE Operating Rule

Or

- When Federal regulation or Federal notices to the industry impacting the transactions addressed by this rule are published.

Substantive changes necessary to the tables will be reviewed and approved by CAQH CORE as necessary to ensure accurate and timely revision. The impact of any such changes to any Phase IV CAQH CORE Infrastructure Rule will be considered during the review of potential revisions. Phase IV CAQH CORE Infrastructure Rules address other requirements for conducting the transactions addressed by this rule, such as response times for Real Time and/or Batch, System Availability, Companion Document flow and format, etc.

3.8 How This Rule Relates to Previous CAQH CORE Operating Rules

The Phase I CAQH CORE 153 Connectivity Rule established the required use of the public Internet. The Phase II CAQH CORE 270 Connectivity Rule extended the Phase I CAQH CORE 153 Connectivity Rule by establishing a Safe Harbor and specifying the connectivity that all HIPAA-covered entities or their agents must implement and support. (See §5) Each of the Phase I and Phase II CAQH CORE rule requirements has been incorporated into this Phase IV Rule except that the MIME Multipart envelope and Username+Password submitter authentication requirements are not retained in this Phase IV CAQH CORE 470 Connectivity Rule v4.0.0. The use of MTOM for SOAP Real Time in this phase implies that use of CDATA tags for SOAP Real Time inline payload, or use of Base64 encoding for payloads with non-printable characters are not a requirement in this phase. Further, relative to Phase II, the SSL/TLS requirements in this phase have been updated (§3.2) to improve support for FIPS 140-2 compliance.

Since this Phase IV CAQH CORE 470 Connectivity Rule v4.0.0 is intended to be independent of both the Phase I CAQH CORE 153 Connectivity Rule and the Phase II CAQH CORE 270 Connectivity Rule and must stand alone on its own merits; implementers of those rules are not required to de-implement or otherwise discontinue support for any of these Phase I and/or Phase II CAQH CORE rules requirements.

While this Phase IV CAQH CORE 470 Connectivity Rule v4.0.0 is mandated for the exchange of transactions addressed in Phase IV CAQH CORE, it may also be used for the exchange of transactions addressed by the previous CAQH CORE Phases (i.e., Phases I, II and III) in accordance with the Safe Harbor provision of the Phase II CAQH CORE 270 Connectivity Rule v2.2.0. However, this does not permit any HIPAA-covered entity or its agent to discontinue support for the exchange of transactions addressed in CORE Phase II and CORE Phase III as required in the Phase II CAQH CORE 270 Connectivity Rule v2.2.0.

3.9 Assumptions

The following assumptions apply to this rule:

- Interoperability, utilization and efficiency will improve by having fewer connectivity/security variations and uniform enveloping standards and metadata.
- This rule is based upon a specific set of open standards and the versions of these standards specified in §3.1. As open standards and versions evolve, appropriate version control practices may need to be applied to keep the Rule consistent with industry best practices with regards to standard versions.

- This rule is a component of the larger set of Phase IV CAQH CORE Operating Rules; as such, all the CAQH CORE Guiding Principles apply to this rule and all other rules.
- All entities seeking voluntary Phase IV CORE Certification will be Phase I, Phase II and Phase III CORE-certified, or concurrently testing for compliance with these rules as they provide a foundation for Phase IV CAQH CORE. The exception is vendors/clearinghouses that do not conduct the ASC X12N v5010 270/271 eligibility, the ASC X12N v5010 276/277 claim status, or the ASC X12N v5010 835 remittance advice transactions.

4 Rule

This section specifies the requirements for transport, message envelope, submitter authentication, envelope metadata and the specifications for SOAP+WSDL. The rationale and business justification for these conformance requirements are described in §2.

4.1 CAQH CORE Message Envelope and Submitter Authentication Requirements

This rule requires HIPAA-covered entities or their agents to support only one set of requirements for message enveloping and one method for submitter authentication in order to reduce variations and enable greater interoperability in the market.)

4.1.1 Message Envelope Requirement

This rule requires the use of SOAP+WSDL (See §4.1.3).

4.1.2 Submitter Authentication Requirement

This rule requires the use of X.509 Client Authentication (mutual authentication) over SSL 3.0 (TLS 1.1 or higher may be used as per the specifications in §3.2).

4.1.3 Specifications for SOAP+WSDL Envelope Standard (normative[71])

This section defines the SOAP+WSDL envelope method for Phase IV CAQH CORE 470 Connectivity Rule v4.0.0. The XML Schema that is defined below is used within the Web Services Definition Language (WSDL) specification.

Note: The terms SOAP, WSDL, MTOM, Normative and Non-normative are defined in *Appendix §7.2: Abbreviations and Definitions used in this Rule*.

4.1.3.1 Phase IV CAQH CORE 470 Connectivity Rule v4.0.0 XML Schema Specification (normative)

The Phase IV CAQH CORE compliant XML Schema Specification file name below is called *CORERule4.0.0.xsd*, and is available at *http://www.caqh.org/sites/default/files/core/wsdl/CORERule4.0.0.xsd*. This schema has ten elements, each representing a type of request or response message envelope:

- Real Time Request Schema (Element name is *COREEnvelopeRealTimeRequest*)
- Real Time Response (Element name is *COREEnvelopeRealTimeResponse*)
- Batch Submission (Element name is *COREEnvelopeBatchSubmission*)
- Batch Submission Response (Element name is *COREEnvelopeBatchSubmissionResponse*)

[71] See §7.2 Abbreviations and Definitions used in this Rule for a definition of Normative.

- Batch Submission Acknowledgement Retrieval Request (Element name is *COREEnvelopeBatchSubmissionAckRetrievalRequest*)
- Batch Submission Acknowledgement Retrieval Response (Element name is *COREEnvelopeBatchSubmissionAckRetrievalResponse*)
- Batch Results Retrieval Request (Element name is *COREEnvelopeBatchResultsRetrievalRequest*)
- Batch Results Retrieval Response (Element name is *COREEnvelopeBatchResultsRetrievalResponse*)

- Batch Results Acknowledgement Submission (Element name is *COREEnvelopeBatchResultsAckSubmission*)
- Batch Results Acknowledgement Submission Response (Element name is *COREEnvelopeBatchResultsAckSubmissionResponse*)

A consequence of the CAQH CORE XML Schema Specification being normative is that any changes to the structure and syntax of the SOAP Body make the implementation non-compliant. Any such implementations must be done under the CAQH CORE Safe Harbor provision.

```
<?xml version="1.0"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns="http://www.caqh.org/SOAP/WSDL/CORERule4.0.0.xsd"
targetNamespace="http://www.caqh.org/SOAP/WSDL/CORERule4.0.0.xsd">
 <xs:element name="COREEnvelopeRealTimeRequest">
  <xs:complexType>
   <xs:sequence>
    <xs:element name="PayloadType" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="ProcessingMode" type="RealTimeMode" minOccurs="1" maxOccurs="1"/>
    <xs:element name="PayloadID" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="TimeStamp" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="SenderID" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="ReceiverID" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="CORERuleVersion" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="Payload" type="xs:base64Binary" minOccurs="1" maxOccurs="1"/>
   </xs:sequence>
  </xs:complexType>
 </xs:element>
 <xs:element name="COREEnvelopeRealTimeResponse">
  <xs:complexType>
   <xs:sequence>
    <xs:element name="PayloadType" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="ProcessingMode" type="RealTimeMode" minOccurs="1" maxOccurs="1"/>
    <xs:element name="PayloadID" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="TimeStamp" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="SenderID" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="ReceiverID" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="CORERuleVersion" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="Payload" type="xs:base64Binary" minOccurs="0" maxOccurs="1"/>
    <xs:element name="ErrorCode" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="ErrorMessage" type="xs:string" minOccurs="1" maxOccurs="1"/>
   </xs:sequence>
  </xs:complexType>
 </xs:element>
 <xs:element name="COREEnvelopeBatchSubmission">
  <xs:complexType>
   <xs:sequence>
    <xs:element name="PayloadType" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="ProcessingMode" type="BatchMode" minOccurs="1" maxOccurs="1"/>
    <xs:element name="PayloadID" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="PayloadLength" type="xs:int" minOccurs="1" maxOccurs="1"/>
    <xs:element name="TimeStamp" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="SenderID" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="ReceiverID" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="CORERuleVersion" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="CheckSum" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="Payload" type="xs:base64Binary" minOccurs="1" maxOccurs="1"/>
   </xs:sequence>
  </xs:complexType>
 </xs:element>
 <xs:element name="COREEnvelopeBatchSubmissionResponse">
  <xs:complexType>
   <xs:sequence>
    <xs:element name="PayloadType" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="ProcessingMode" type="BatchMode" minOccurs="1" maxOccurs="1"/>
    <xs:element name="PayloadID" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="PayloadLength" type="xs:int" minOccurs="0" maxOccurs="1"/>
    <xs:element name="TimeStamp" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="SenderID" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="ReceiverID" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="CORERuleVersion" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="CheckSum" type="xs:string" minOccurs="0" maxOccurs="1"/>
    <xs:element name="Payload" type="xs:base64Binary" minOccurs="0" maxOccurs="1"/>
    <xs:element name="ErrorCode" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="ErrorMessage" type="xs:string" minOccurs="1" maxOccurs="1"/>
   </xs:sequence>
  </xs:complexType>
 </xs:element>
 <xs:element name="COREEnvelopeBatchSubmissionAckRetrievalRequest">
```

```
  <xs:complexType>
   <xs:sequence>
    <xs:element name="PayloadType" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="ProcessingMode" type="BatchMode" minOccurs="1" maxOccurs="1"/>
    <xs:element name="PayloadID" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="PayloadLength" type="xs:int" minOccurs="0" maxOccurs="1"/>
    <xs:element name="TimeStamp" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="SenderID" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="ReceiverID" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="CORERuleVersion" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="CheckSum" type="xs:string" minOccurs="0" maxOccurs="1"/>
    <xs:element name="Payload" type="xs:base64Binary" minOccurs="0" maxOccurs="1"/>
   </xs:sequence>
  </xs:complexType>
 </xs:element>
 <xs:element name="COREEnvelopeBatchSubmissionAckRetrievalResponse">
  <xs:complexType>
   <xs:sequence>
    <xs:element name="PayloadType" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="ProcessingMode" type="BatchMode" minOccurs="1" maxOccurs="1"/>
    <xs:element name="PayloadID" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="PayloadLength" type="xs:int" minOccurs="0" maxOccurs="1"/>
    <xs:element name="TimeStamp" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="SenderID" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="ReceiverID" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="CORERuleVersion" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="CheckSum" type="xs:string" minOccurs="0" maxOccurs="1"/>
    <xs:element name="Payload" type="xs:base64Binary" minOccurs="0" maxOccurs="1"/>
    <xs:element name="ErrorCode" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="ErrorMessage" type="xs:string" minOccurs="1" maxOccurs="1"/>
   </xs:sequence>
  </xs:complexType>
 </xs:element>
 <xs:element name="COREEnvelopeBatchResultsRetrievalRequest">
  <xs:complexType>
   <xs:sequence>
    <xs:element name="PayloadType" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="ProcessingMode" type="BatchMode" minOccurs="1" maxOccurs="1"/>
    <xs:element name="PayloadID" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="PayloadLength" type="xs:int" minOccurs="0" maxOccurs="1"/>
    <xs:element name="TimeStamp" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="SenderID" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="ReceiverID" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="CORERuleVersion" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="CheckSum" type="xs:string" minOccurs="0" maxOccurs="1"/>
    <xs:element name="Payload" type="xs:base64Binary" minOccurs="0" maxOccurs="1"/>
   </xs:sequence>
  </xs:complexType>
 </xs:element>
 <xs:element name="COREEnvelopeBatchResultsRetrievalResponse">
  <xs:complexType>
   <xs:sequence>
    <xs:element name="PayloadType" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="ProcessingMode" type="BatchMode" minOccurs="1" maxOccurs="1"/>
    <xs:element name="PayloadID" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="PayloadLength" type="xs:int" minOccurs="0" maxOccurs="1"/>
    <xs:element name="TimeStamp" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="SenderID" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="ReceiverID" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="CORERuleVersion" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="CheckSum" type="xs:string" minOccurs="0" maxOccurs="1"/>
    <xs:element name="Payload" type="xs:base64Binary" minOccurs="0" maxOccurs="1"/>
    <xs:element name="ErrorCode" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="ErrorMessage" type="xs:string" minOccurs="1" maxOccurs="1"/>
   </xs:sequence>
  </xs:complexType>
 </xs:element>
 <xs:element name="COREEnvelopeBatchResultsAckSubmission">
  <xs:complexType>
   <xs:sequence>
    <xs:element name="PayloadType" type="xs:string" minOccurs="1" maxOccurs="1"/>
```

```
    <xs:element name="ProcessingMode" type="BatchMode" minOccurs="1" maxOccurs="1"/>
    <xs:element name="PayloadID" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="PayloadLength" type="xs:int" minOccurs="0" maxOccurs="1"/>
    <xs:element name="TimeStamp" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="SenderID" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="ReceiverID" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="CORERuleVersion" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="CheckSum" type="xs:string" minOccurs="0" maxOccurs="1"/>
    <xs:element name="Payload" type="xs:base64Binary" minOccurs="0" maxOccurs="1"/>
   </xs:sequence>
  </xs:complexType>
 </xs:element>
 <xs:element name="COREEnvelopeBatchResultsAckSubmissionResponse">
  <xs:complexType>
   <xs:sequence>
    <xs:element name="PayloadType" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="ProcessingMode" type="BatchMode" minOccurs="1" maxOccurs="1"/>
    <xs:element name="PayloadID" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="PayloadLength" type="xs:int" minOccurs="0" maxOccurs="1"/>
    <xs:element name="TimeStamp" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="SenderID" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="ReceiverID" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="CORERuleVersion" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="CheckSum" type="xs:string" minOccurs="0" maxOccurs="1"/>
    <xs:element name="Payload" type="xs:base64Binary" minOccurs="0" maxOccurs="1"/>
    <xs:element name="ErrorCode" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="ErrorMessage" type="xs:string" minOccurs="1" maxOccurs="1"/>
   </xs:sequence>
  </xs:complexType>
 </xs:element>
 <xs:simpleType name="RealTimeMode">
  <xs:restriction base="xs:string">
   <xs:pattern value="RealTime"/>
  </xs:restriction>
 </xs:simpleType>
 <xs:simpleType name="BatchMode">
  <xs:restriction base="xs:string">
   <xs:pattern value="Batch"/>
  </xs:restriction>
 </xs:simpleType>
</xs:schema>
```

4.1.3.2 CAQH CORE Connectivity Web Services Definition Language (WSDL) Specification (normative)

The Phase IV CAQH CORE 470 Connectivity Rule v4.0.0 Web Services Definition Language (WSDL) file below is called *CORERule4.0.0.wsdl*, and is available at *http://www.caqh.org/sites/default/files/core/wsdl/CORERule4.0.0.wsdl*. The WSDL below makes use of the XML Schema (*CORERule4.0.0.xsd*) as specified in §4.1.3.1. Within this WSDL the following types of messages are defined:

- Real Time Request Message (Message name is *RealTimeRequestMessage*)
- Real Time Response Message (Message name is *RealTimeResponseMessage*)
- Batch Submission Request Message (Message name is *BatchSubmissionMessage*)
- Batch Submission Response Message (Message name is *BatchSubmissionResponseMessage*)
- Batch Submission Acknowledgement Retrieval Request (Message name is *BatchSubmissionAckRetrievalRequestMessage*)
- Batch Submission Acknowledgement Retrieval Response (Message name is *BatchSubmissionAckRetrievalResponseMessage*)
- Batch Results Retrieval Request Message (Message name is *BatchResultsRetrievalRequestMessage*)
- Batch Results Retrieval Response Message (Message name is *BatchResultsRetrievalResponseMessage*)

- Batch Results Acknowledgement Submission Message (Message name is *BatchResultsAckSubmissionMessage*)
- Batch Results Acknowledgement Submission Response Message (Message name is *BatchResultsAckSubmissionResponseMessage*)

Using the above message definitions, the following types of transactions are defined:

- Real Time Transaction (Operation name is *RealTimeTransaction*)
- Batch Submit Transaction (Operation name is *BatchSubmitTransaction*)
- Batch Submit Acknowledgement Retrieval Transaction (Operation name is *BatchSubmitAckRetrievalTransaction*)
- Batch Results Retrieval Transaction (Operation name is *BatchResultsRetrievalTransaction*)
- Batch Results Acknowledgement Transaction (Operation name is *BatchResultsAckSubmitTransaction*)
- Generic Batch Submission Transaction (Operation name is *GenericBatchSubmissionTransaction*)
- Generic Batch Submission Acknowledgment Retrieval Transaction (Operation name is *GenericBatchSubmissionAckRetrievalTransaction*)
- Generic Batch Retrieval Transaction (Operation name is *GenericBatchRetrievalTransaction)*
- Generic Batch Receipt Confirmation Transaction (Operation name is *GenericBatchReceiptConfirmationTransaction)*

The CAQH CORE Connectivity WSDL uses an implicit style of specification, which allows the optional use of additional elements within the SOAP Header. Server entities that require the use of SOAP Header elements must define their use in the entity's Connectivity Companion Document. Client or Server entities that do not use these SOAP Header elements must ignore them.

```
<?xml version="1.0" encoding="UTF-8"?>
<wsdl:definitions xmlns:CORE="http://www.caqh.org/SOAP/WSDL/"
                              xmlns:soap12="http://schemas.xmlsoap.org/wsdl/soap12/"
                              xmlns:xsd="http://www.w3.org/2001/XMLSchema"
                              xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
                              xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
                              xmlns:CORE-XSD="http://www.caqh.org/SOAP/WSDL/CORERule4.0.0.xsd"
                              xmlns="http://schemas.xmlsoap.org/wsdl/"
                              name="CORE"
                              targetNamespace="http://www.caqh.org/SOAP/WSDL/">

 <!-- TYPES (BEGIN) -->
 <wsdl:types>
  <xsd:schema xmlns="http://schemas.xmlsoap.org/wsdl/"
                                      elementFormDefault="qualified"
targetNamespace="http://www.caqh.org/SOAP/WSDL/">
   <xsd:import namespace="http://www.caqh.org/SOAP/WSDL/CORERule4.0.0.xsd"
schemaLocation="CORERule4.0.0.xsd"/>
  </xsd:schema>
 </wsdl:types>
 <!-- TYPES (END) -->

 <!-- MESSAGE (BEGIN) -->
 <wsdl:message name="RealTimeRequestMessage">
  <wsdl:part name="body" element="CORE-XSD:COREEnvelopeRealTimeRequest"/>
 </wsdl:message>
 <wsdl:message name="RealTimeResponseMessage">
  <wsdl:part name="body" element="CORE-XSD:COREEnvelopeRealTimeResponse"/>
 </wsdl:message>
 <wsdl:message name="BatchSubmissionMessage">
  <wsdl:part name="body" element="CORE-XSD:COREEnvelopeBatchSubmission"/>
 </wsdl:message>
```

```
<wsdl:message name="BatchSubmissionResponseMessage">
 <wsdl:part name="body" element="CORE-XSD:COREEnvelopeBatchSubmissionResponse"/>
</wsdl:message>
<wsdl:message name="BatchSubmissionAckRetrievalRequestMessage">
 <wsdl:part name="body"
       element="CORE-XSD:COREEnvelopeBatchSubmissionAckRetrievalRequest"/>
</wsdl:message>
<wsdl:message name="BatchSubmissionAckRetrievalResponseMessage">
 <wsdl:part name="body"
      element="CORE-XSD:COREEnvelopeBatchSubmissionAckRetrievalResponse"/>
</wsdl:message>
<wsdl:message name="BatchResultsRetrievalRequestMessage">
 <wsdl:part name="body"
         element="CORE-XSD:COREEnvelopeBatchResultsRetrievalRequest"/>
</wsdl:message>
<wsdl:message name="BatchResultsRetrievalResponseMessage">
 <wsdl:part name="body"
         element="CORE-XSD:COREEnvelopeBatchResultsRetrievalResponse"/>
</wsdl:message>
<wsdl:message name="BatchResultsAckSubmissionMessage">
 <wsdl:part name="body" element="CORE-XSD:COREEnvelopeBatchResultsAckSubmission"/>
</wsdl:message>
<wsdl:message name="BatchResultsAckSubmissionResponseMessage">
 <wsdl:part name="body" element="CORE-XSD:COREEnvelopeBatchResultsAckSubmissionResponse"/>
</wsdl:message>
<!-- MESSAGE (END) -->

<!-- PORTTYPE (BEGIN) -->
<wsdl:portType name="CORETransactions">

 <!-- OPERATION: REAL TIME INTERACTION (BEGIN) -->
 <wsdl:operation name="RealTimeTransaction">
  <wsdl:input message="CORE:RealTimeRequestMessage"/>
  <wsdl:output message="CORE:RealTimeResponseMessage"/>
 </wsdl:operation>
 <!-- OPERATION: REAL TIME INTERACTION (END) -->

 <!-- OPERATION: BATCH INTERACTION (BEGIN) -->
 <wsdl:operation name="BatchSubmitTransaction">
  <wsdl:input message="CORE:BatchSubmissionMessage"/>
  <wsdl:output message="CORE:BatchSubmissionResponseMessage"/>
 </wsdl:operation>
 <wsdl:operation name="BatchSubmitAckRetrievalTransaction">
  <wsdl:input message="CORE:BatchSubmissionAckRetrievalRequestMessage"/>
  <wsdl:output message="CORE:BatchSubmissionAckRetrievalResponseMessage"/>
 </wsdl:operation>
 <wsdl:operation name="BatchResultsRetrievalTransaction">
  <wsdl:input message="CORE:BatchResultsRetrievalRequestMessage"/>
  <wsdl:output message="CORE:BatchResultsRetrievalResponseMessage"/>
 </wsdl:operation>
 <wsdl:operation name="BatchResultsAckSubmitTransaction">
  <wsdl:input message="CORE:BatchResultsAckSubmissionMessage"/>
  <wsdl:output message="CORE:BatchResultsAckSubmissionResponseMessage"/>
 </wsdl:operation>
 <!-- OPERATION: BATCH INTERACTION (END) -->

 <!-- OPERATION: GENERIC PUSH (BEGIN) -->
 <wsdl:operation name="GenericBatchSubmissionTransaction">
  <wsdl:input message="CORE:BatchSubmissionMessage"/>
  <wsdl:output message="CORE:BatchSubmissionResponseMessage"/>
 </wsdl:operation>
  <wsdl:operation name="GenericBatchSubmissionAckRetrievalTransaction”>
   <wsdl:input message="CORE:BatchSubmissionAckRetrievalRequestMessage"/>
   <wsdl:output message="CORE:BatchSubmissionAckRetrievalResponseMessage”/>
 </wsdl:operation>
 <!-- OPERATION: GENERIC PUSH (END) -->

 <!-- OPERATION: GENERIC PULL (BEGIN) -->
 <wsdl:operation name="GenericBatchRetrievalTransaction">
  <wsdl:input message="CORE:BatchResultsRetrievalRequestMessage"/>
  <wsdl:output message="CORE:BatchResultsRetrievalResponseMessage"/>
```

```
  </wsdl:operation>
  <wsdl:operation name="GenericBatchReceiptConfirmationTransaction">
   <wsdl:input message="CORE:BatchResultsAckSubmissionMessage"/>
   <wsdl:output message="CORE:BatchResultsAckSubmissionResponseMessage"/>
  </wsdl:operation>
  <!-- OPERATION: GENERIC PULL (END) -->
 </wsdl:portType>
 <!-- PORTTYPE (END) -->

 <!-- BINDING (BEGIN) -->
 <wsdl:binding name="CoreSoapBinding" type="CORE:CORETransactions">
  <soap12:binding style="document" transport="http://schemas.xmlsoap.org/soap/http"/>

  <!-- OPERATION: REAL TIME TRANSACTION (BEGIN) -->
  <wsdl:operation name="RealTimeTransaction">
   <soap12:operation soapAction="RealTimeTransaction" style="document"/>
   <wsdl:input>
    <soap12:body use="literal"/>
   </wsdl:input>
   <wsdl:output>
    <soap12:body use="literal"/>
   </wsdl:output>
  </wsdl:operation>
  <!-- OPERATION: REAL TIME TRANSACTION (END) -->

  <!-- OPERATION: BATCH TRANSACTION (BEGIN) -->
  <wsdl:operation name="BatchSubmitTransaction">
   <soap12:operation soapAction="BatchSubmitTransaction" style="document"/>
   <wsdl:input>
    <soap12:body use="literal"/>
   </wsdl:input>
   <wsdl:output>
    <soap12:body use="literal"/>
   </wsdl:output>
  </wsdl:operation>
  <wsdl:operation name="BatchSubmitAckRetrievalTransaction">
   <soap12:operation soapAction="BatchSubmitAckRetrievalTransaction" style="document"/>
   <wsdl:input>
    <soap12:body use="literal"/>
   </wsdl:input>
   <wsdl:output>
    <soap12:body use="literal"/>
   </wsdl:output>
  </wsdl:operation>
  <wsdl:operation name="BatchResultsRetrievalTransaction">
   <soap12:operation soapAction="BatchResultsRetrievalTransaction" style="document"/>
   <wsdl:input>
    <soap12:body use="literal"/>
   </wsdl:input>
   <wsdl:output>
    <soap12:body use="literal"/>
   </wsdl:output>
  </wsdl:operation>
  <wsdl:operation name="BatchResultsAckSubmitTransaction">
   <soap12:operation soapAction="BatchResultsAckSubmitTransaction" style="document"/>
   <wsdl:input>
    <soap12:body use="literal"/>
   </wsdl:input>
   <wsdl:output>
    <soap12:body use="literal"/>
   </wsdl:output>
  </wsdl:operation>
  <!-- OPERATION: BATCH TRANSACTION (END) -->

  <!-- OPERATION: GENERIC PUSH (BEGIN) -->
  <wsdl:operation name="GenericBatchSubmissionTransaction">
   <soap12:operation soapAction="GenericBatchSubmissionTransaction" style="document"/>
   <wsdl:input>
    <soap12:body use="literal"/>
   </wsdl:input>
   <wsdl:output>
```

```
    <soap12:body use="literal"/>
   </wsdl:output>
  </wsdl:operation>
  <wsdl:operation name="GenericBatchSubmissionAckRetrievalTransaction">
   <soap12:operation soapAction="GenericBatchSubmissionAckRetrievalTransaction" style="document"/>
   <wsdl:input>
    <soap12:body use="literal"/>
   </wsdl:input>
   <wsdl:output>
    <soap12:body use="literal"/>
   </wsdl:output>
  </wsdl:operation>
  <!-- OPERATION: GENERIC PUSH (END) -->

  <!-- OPERATION: GENERIC PULL (BEGIN) -->
  <wsdl:operation name="GenericBatchRetrievalTransaction">
   <soap12:operation soapAction="GenericBatchRetrievalTransaction" style="document"/>
   <wsdl:input>
    <soap12:body use="literal"/>
   </wsdl:input>
   <wsdl:output>
    <soap12:body use="literal"/>
   </wsdl:output>
  </wsdl:operation>
   <wsdl:operation name="GenericBatchReceiptConfirmationTransaction">
   <soap12:operation soapAction="GenericBatchReceiptConfirmationTransaction" style="document"/>
   <wsdl:input>
    <soap12:body use="literal"/>
   </wsdl:input>
   <wsdl:output>
    <soap12:body use="literal"/>
   </wsdl:output>
  </wsdl:operation>
  <!-- OPERATION: GENERIC PULL (END) -->

 </wsdl:binding>
 <!-- BINDING (END) -->

 <!-- SERVICE (BEGIN) -->
 <wsdl:service name="Core">
  <wsdl:port name="CoreSoapPort" binding="CORE:CoreSoapBinding">
   <soap12:address location="http://URL_OF_WEB_SERVICE"/>
  </wsdl:port>
 </wsdl:service>
 <!-- SERVICE (END) -->

</wsdl:definitions>
```

The following sections show Request and Response messages using the SOAP envelope, based on the WSDL schemas defined above. The SOAP Real Time Request/Response examples below are non-normative[72]. They are based on the real-world examples provided by CAQH CORE Participating Organizations, but have been updated to use the CAQH CORE-required metadata that is part of Phase IV CAQH CORE 470 Connectivity Rule v4.0.0.

*4.1.3.3 **Real Time Request Message Structure (non-normative)***

The Real Time Request message structure shown below specifies SOAP 1.2.

SOAP Version 1.2 must be implemented by all Servers.

This shows the following components:

1. The HTTP Headers are shown colored in blue.

[72] A non-normative description is informational only. See §7.2 Abbreviations and Definitions Used in this Rule.

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

3. The Real Time Payload file (MTOM attachment) is shown colored in orange.

```
POST /CORE/PriorAuthRealTime HTTP/1.1
Host: server_host:server_port
Content-Type: multipart/related; boundary= MIMEBoundaryurn_uuid_5117AAE1116EA8B87A1200060184614;
type="application/xop+xml"; start="0.urn:uuid:5117AAE1116EA8B87A1200060184615"; start-
info="application/soap+xml";
action="http://www.caqh.org/SOAP/WSDL/CORETransactions/RealTimeTransaction"

--MIMEBoundaryurn_uuid_5117AAE1116EA8B87A1200060184614
Content-Type: application/xop+xml; charset=UTF-8; type="application/soap+xml"
Content-Transfer-Encoding: binary
Content-ID: <0.urn:uuid:5117AAE1116EA8B87A1200060184615>

<soapenv:Envelope xmlns:soapenv="http://www.w3.org/2003/05/soap-envelope">
        <soapenv:Body>
              <ns1:COREEnvelopeRealTimeRequest
              xmlns:ns1="http://www.caqh.org/SOAP/WSDL/CORERule4.0.0.xsd">
               <PayloadType>X12_278_Request_005010X217E1_2</PayloadType>
                      <ProcessingMode>RealTime</ProcessingMode>
                      <PayloadID>f81d4fae-7dec-11d0-a765-00a0c91e6bf6</PayloadID>
                      <TimeStamp>2007-08-30T10:20:34Z</TimeStamp>
                      <SenderID>HospitalA</SenderID>
                      <ReceiverID>PayerB</ReceiverID>
                      <CORERuleVersion>4.0.0</CORERuleVersion>
            <Payload>
                       <xop:Include href="cid:1.urn:uuid:5117AAE1116EA8B87A1200060184692"
                      xmlns:xop="http://www.w3.org/2004/08/xop/include" />
            </Payload>
              </ns1:COREEnvelopeRealTimeRequest>
               </soapenv:Body>
</soapenv:Envelope>

--MIMEBoundaryurn_uuid_5117AAE1116EA8B87A1200060184614
Content-Type: image/jpeg
Content-Transfer-Encoding: binary
Content-ID: <1.urn:uuid:5117AAE1116EA8B87A1200060184692>

<Real Time Request Payload (e.g., a payload of type X12_278_Request_005010X217E1_2) goes here>

--MIMEBoundaryurn_uuid_5117AAE1116EA8B87A1200060184614--
```

*4.1.3.4 **Real Time Response Message Structure (non-normative)***

The Real Time Response message structure shown below specifies SOAP 1.2. The HTTP Header is shown in blue. The remainder of the request is the SOAP Envelope. The portion of the SOAP envelope colored in green has the metadata that is defined as part of the Phase IV CAQH CORE Connectivity Rule v4.0.0. (See §4.4)

```
HTTP/1.1 200 OK
Content-Type: multipart/related; boundary= MIMEBoundaryurn_uuid_5117AAE1116EA8B87A1200060184614;
type="application/xop+xml"; start="0.urn:uuid:5117AAE1116EA8B87A1200060184615"; start-
info="application/soap+xml";
action="http://www.caqh.org/SOAP/WSDL/CORETransactions/RealTimeTransactionResponse"

--MIMEBoundaryurn_uuid_5117AAE1116EA8B87A1200060184614
Content-Type: application/xop+xml; charset=UTF-8; type="application/soap+xml"
Content-Transfer-Encoding: binary
Content-ID: <0.urn:uuid:5117AAE1116EA8B87A1200060184615>

<soapenv:Envelope xmlns:soapenv="http://www.w3.org/2003/05/soap-envelope">
       <soapenv:Body>
              <ns1:COREEnvelopeRealTimeResponse
              xmlns:ns1="http://www.caqh.org/SOAP/WSDL/CORERule4.0.0.xsd">
                     <PayloadType>X12_278_Response_005010X217E1_2</PayloadType>
                     <ProcessingMode>RealTime</ProcessingMode>
                     <PayloadID>a81d44ae-7dec-11d0-a765-00a0c91e6ba0</PayloadID>
                     <TimeStamp>2007-08-30T10:20:34Z</TimeStamp>
                     <SenderID>PayerB</SenderID>
                     <ReceiverID>HospitalA</ReceiverID>
                     <CORERuleVersion>4.0.0</CORERuleVersion>
            <Payload>
                     <xop:Include href="cid:1.urn:uuid:5117AAE1116EA8B87A1200060184692"
                     xmlns:xop="http://www.w3.org/2004/08/xop/include" />
            </Payload>
                     <ErrorCode>Success</ErrorCode>
                     <ErrorMessage></ErrorMessage>
              </ns1:COREEnvelopeRealTimeResponse>
        </soapenv:Body>
 </soapenv:Envelope>

--MIMEBoundaryurn_uuid_5117AAE1116EA8B87A1200060184614
Content-Type: image/jpeg
Content-Transfer-Encoding: binary
Content-ID: <1.urn:uuid:5117AAE1116EA8B87A1200060184692>

<Real Time Response Payload (e.g., a payload of type X12_278_Response_005010X217E1_2) goes here>

--MIMEBoundaryurn_uuid_5117AAE1116EA8B87A1200060184614--
```

*4.1.3.5 **Batch Submission Message (non-normative)***[73]

The Batch Submission message structure shown below specifies SOAP 1.2, and also uses MTOM (See §7.1) to send the payload file. This shows the following:

1. The HTTP Headers are shown colored in blue.
2. The portion of the SOAP envelope colored in green has the metadata that is defined as part of the Phase IV CAQH CORE Connectivity Rule v4.0.0. (See §4.4)
3. The Batch file (MTOM attachment) is shown colored in orange.

[73] The Batch Payload Submission in a Generic Push interaction (i.e., Step 1 in the sequence diagram shown in §7.3.3.1) uses the same request message as the Batch Submission Request message structure depicted below, with *PayloadType* values based on what is being submitted.

```
POST /CORE/PriorAuthBatch HTTP/1.1
Content-Type: multipart/related; boundary=MIMEBoundaryurn_uuid_5117AAE1116EA8B87A1200060184614;
type="application/xop+xml"; start="0.urn:uuid:5117AAE1116EA8B87A1200060184615@apache.org"; start-
info="application/soap+xml"; action="BatchSubmitTransaction"

--MIMEBoundaryurn_uuid_5117AAE1116EA8B87A1200060184614
Content-Type: application/xop+xml; charset=UTF-8; type="application/soap+xml"
Content-Transfer-Encoding: binary
Content-ID: <0.urn:uuid:5117AAE1116EA8B87A1200060184615@apache.org>

<soapenv:Envelope xmlns:soapenv="http://www.w3.org/2003/05/soap-envelope">
       <soapenv:Body>
              <ns1:COREEnvelopeBatchSubmission
              xmlns:ns1="http://www.caqh.org/SOAP/WSDL/CORERule4.0.0.xsd">
                      <PayloadType>X12_278_Request_005010X217E1_2</PayloadType>
                      <ProcessingMode>Batch</ProcessingMode>
                      <PayloadID>f81d4fae-7dec-11d0-a765-00a0c91e6bf6</PayloadID>
                      <PayloadLength>1551254</PayloadLength>
                      <TimeStamp>2007-08-30T10:20:34Z</TimeStamp>
                      <SenderID>HospitalA</SenderID>
                      <ReceiverID>PayerB</ReceiverID>
                      <CORERuleVersion>4.0.0</CORERuleVersion>
                      <CheckSum>43B8485AB5</CheckSum>
                     <Payload>
                     <xop:Include href="cid:1.urn:uuid:5117AAE1116EA8B87A1200060184692@apache.org"
                     xmlns:xop="http://www.w3.org/2004/08/xop/include" />
                      </Payload>
               </ns1:COREEnvelopeBatchSubmission>
        </soapenv:Body>
 </soapenv:Envelope>

--MIMEBoundaryurn_uuid_5117AAE1116EA8B87A1200060184614
Content-Type: image/jpeg
Content-Transfer-Encoding: binary
Content-ID: <1.urn:uuid:5117AAE1116EA8B87A1200060184692@apache.org>

<Mixed batch file>

--MIMEBoundaryurn_uuid_5117AAE1116EA8B87A1200060184614--
```

*4.1.3.6 **Batch Submission Response Message (non-normative)***[74]

The Batch Submission Response message structure shown below specifies SOAP 1.2 and MTOM. This shows the following:

1. The HTTP Headers are shown colored in blue.
2. The portion of the SOAP envelope colored in green has the metadata that is defined as part of the Phase IV CAQH CORE Connectivity Rule v4.0.0. (See §4.4)

[74] The response to Batch Payload submission in a Generic Push interaction (i.e., Step 2 in the sequence diagram in §7.3.3.1) uses the same response message as the Batch Submission Response message structure depicted below, with PayloadType values based on the response to what is being submitted.

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: multipart/related; boundary=MIMEBoundaryurn_uuid_0B72121B1FEFA9BDD31200060195339;
type="application/xop+xml"; start="0.urn:uuid:0B72121B1FEFA9BDD31200060195340@apache.org"; start-
info="application/soap+xml";
action="http://www.caqh.org/SOAP/WSDL/CORETransactions/BatchSubmitTransactionResponse"

--MIMEBoundaryurn_uuid_0B72121B1FEFA9BDD31200060195339
Content-Type: application/xop+xml; charset=UTF-8; type="application/soap+xml"
Content-Transfer-Encoding: binary
Content-ID: <0.urn:uuid:0B72121B1FEFA9BDD31200060195340@apache.org>

<soapenv:Envelope xmlns:soapenv="http://www.w3.org/2003/05/soap-envelope">
        <soapenv:Body>
              <ns1:COREEnvelopeBatchSubmissionResponse
              xmlns:ns1="http://www.caqh.org/SOAP/WSDL/CORERule4.0.0.xsd">
                    <PayloadType>X12_BatchReceiptConfirmation</PayloadType>
                    <ProcessingMode>Batch</ProcessingMode>
                    <PayloadID>f81d4fae-7dec-11d0-a765-00a0c91e6bf6</PayloadID>
                    <TimeStamp>2007-08-30T10:20:34Z</TimeStamp>
                    <SenderID>PayerB</SenderID>
                    <ReceiverID>HospitalA</ReceiverID>
                    <CORERuleVersion>4.0.0</CORERuleVersion>
                    <ErrorCode>Success</ErrorCode>
                    <ErrorMessage></ErrorMessage>
               </ns1:COREEnvelopeBatchSubmissionResponse>
        </soapenv:Body>
 </soapenv:Envelope>

--MIMEBoundaryurn_uuid_0B72121B1FEFA9BDD31200060195339--
```

*4.1.3.7 **Batch Submission Acknowledgement Retrieval Request Message (non-normative)***

The Batch Submission Acknowledgement Retrieval Request message structure shown below specifies SOAP 1.2. The use of MTOM in Batch mode request/response creates multipart MIME even though there is no payload. This shows the following:

1. The HTTP Headers are shown colored in blue.
2. The portion of the SOAP envelope colored in green has the metadata that is defined as part of the Phase IV CAQH CORE Connectivity Rule v4.0.0. (See §4.4)

```
POST /CORE/PriorAuthBatch HTTP/1.1
Content-Type: multipart/related; boundary=MIMEBoundaryurn_uuid_5117AAE1116EA8B87A1200060184614;
type="application/xop+xml"; start="0.urn:uuid:5117AAE1116EA8B87A1200060184615@apache.org"; start-
info="application/soap+xml"; action="BatchSubmitAckRetrievalTransaction"

--MIMEBoundaryurn_uuid_5117AAE1116EA8B87A1200060184614
Content-Type: application/xop+xml; charset=UTF-8; type="application/soap+xml"
Content-Transfer-Encoding: binary
Content-ID: <0.urn:uuid:5117AAE1116EA8B87A1200060184615@apache.org>

<soapenv:Envelope xmlns:soapenv="http://www.w3.org/2003/05/soap-envelope">
       <soapenv:Body>
              <ns1:COREEnvelopeBatchSubmissionAckRetrievalRequest
              xmlns:ns1="http://www.caqh.org/SOAP/WSDL/CORERule4.0.0.xsd">
                     <PayloadType>X12_999_RetrievalRequest_005010X231A1</PayloadType>
                     <ProcessingMode>Batch</ProcessingMode>
                     <PayloadID>f81d4fae-7dec-11d0-a765-00a0c91e6bf6</PayloadID>
                     <TimeStamp>2007-08-30T10:20:34Z</TimeStamp>
                     <SenderID>HospitalA</SenderID>
                     <ReceiverID>PayerB</ReceiverID>
                     <CORERuleVersion>4.0.0</CORERuleVersion>
              </ns1:COREEnvelopeBatchSubmissionAckRetrievalRequest>
       </soapenv:Body>
 </soapenv:Envelope>
--MIMEBoundaryurn_uuid_5117AAE1116EA8B87A1200060184614--
```

*4.1.3.8 **Batch Submission Acknowledgement Retrieval Response Message (non-normative)***[75]

The Batch Submission Acknowledgement Retrieval Response message structure shown below specifies SOAP 1.2 and MTOM. This shows the following:

1. The HTTP Headers are shown colored in blue.
2. The portion of the SOAP envelope colored in green has the metadata that is defined as part of the Phase IV CAQH CORE Connectivity Rule v4.0.0. (See §4.4)
3. The MTOM Attachment is colored in orange.

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: multipart/related; boundary=MIMEBoundaryurn_uuid_0B72121B1FEFA9BDD31200060195339;
type="application/xop+xml"; start="0.urn:uuid:0B72121B1FEFA9BDD31200060195340@apache.org"; start-
info="application/soap+xml"; action="BatchSubmitAckRetrievalTransaction"

--MIMEBoundaryurn_uuid_0B72121B1FEFA9BDD31200060195339
Content-Type: application/xop+xml; charset=UTF-8; type="application/soap+xml"
Content-Transfer-Encoding: binary
Content-ID: <0.urn:uuid:0B72121B1FEFA9BDD31200060195340@apache.org>

<soapenv:Envelope xmlns:soapenv="http://www.w3.org/2003/05/soap-envelope">
        <soapenv:Body>
              <ns1:COREEnvelopeBatchSubmissionAckRetrievalResponse
              xmlns:ns1="http://www.caqh.org/SOAP/WSDL/CORERule4.0.0.xsd">
                     <PayloadType>X12_999_Response_005010X231A1</PayloadType>
                     <ProcessingMode>Batch</ProcessingMode>
                     <PayloadID>f81d4fae-7dec-11d0-a765-00a0c91e6bf6</PayloadID>
                     <PayloadLength>1551254</PayloadLength>
                     <TimeStamp>2007-08-30T10:20:34Z</TimeStamp>
                     <SenderID>PayerB</SenderID>
                     <ReceiverID>HospitalA</ReceiverID>
                     <CORERuleVersion>4.0.0</CORERuleVersion>
                     <CheckSum>43B8485AB5</CheckSum>
                     <Payload>
                    <xop:Include href="cid:1.urn:uuid:5117AAE1116EA8B87A1200060184692@apache.org"
                    xmlns:xop="http://www.w3.org/2004/08/xop/include" />
```

[75] Although this example shows an ASC X12 v5010 999 payload type being sent as a response from a server to the client, this could also include an ASC X12 v5010 TA1. Alternatively, the server may elect to send only an ASC X12 v5010 TA1 without any functional group.

```
                        </Payload>
                        <ErrorCode>Success</ErrorCode>
                        <ErrorMessage></ErrorMessage>
                 </ns1:COREEnvelopeBatchSubmissionAckRetrievalResponse>
        </soapenv:Body>
 </soapenv:Envelope>

--MIMEBoundaryurn_uuid_0B72121B1FEFA9BDD31200060195339
Content-Type: image/jpeg
Content-Transfer-Encoding: binary
Content-ID: <1.urn:uuid:5117AAE1116EA8B87A1200060184692@apache.org>

<999 file>

--MIMEBoundaryurn_uuid_0B72121B1FEFA9BDD31200060195339--
```

*4.1.3.9 **Batch Results Retrieval Request Message (non-normative)**[76]*

The Batch Results Retrieval Request message structure shown below specifies SOAP 1.2. The use of MTOM in Batch Mode request/response creates multipart MIME even though there is no payload (which may be the case for a Batch Retrieval Request). This shows the following:

1. The HTTP Headers are shown colored in blue.
2. The portion of the SOAP envelope colored in green has the metadata that is defined as part of the Phase IV CAQH CORE Connectivity Rule v4.0.0. (See §4.4)

```
POST /CORE/PriorAuthBatch HTTP/1.1
Content-Type: multipart/related; boundary=MIMEBoundaryurn_uuid_5117AAE1116EA8B87A1200060184614;
type="application/xop+xml"; start="0.urn:uuid:5117AAE1116EA8B87A1200060184615@apache.org"; start-
info="application/soap+xml"; action="BatchResultsRetrievalTransaction"

--MIMEBoundaryurn_uuid_5117AAE1116EA8B87A1200060184614
Content-Type: application/xop+xml; charset=UTF-8; type="application/soap+xml"
Content-Transfer-Encoding: binary
Content-ID: <0.urn:uuid:5117AAE1116EA8B87A1200060184615@apache.org>

<soapenv:Envelope xmlns:soapenv="http://www.w3.org/2003/05/soap-envelope">
       <soapenv:Body>
              <ns1:COREEnvelopeBatchResultsRetrievalRequest
              xmlns:ns1="http://www.caqh.org/SOAP/WSDL/CORERule4.0.0.xsd">
        <PayloadType>X12_278_Request_Batch_Results_005010X217E1_2</PayloadType>
                        <ProcessingMode>Batch</ProcessingMode>
                        <PayloadID>f81d4fae-7dec-11d0-a765-00a0c91e6bf6</PayloadID>
                        <TimeStamp>2007-08-30T10:20:34Z</TimeStamp>
                        <SenderID>HospitalA</SenderID>
                        <ReceiverID>PayerB</ReceiverID>
                        <CORERuleVersion>4.0.0</CORERuleVersion>
                 </ns1:COREEnvelopeBatchResultsRetrievalRequest>
        </soapenv:Body>
 </soapenv:Envelope>
--MIMEBoundaryurn_uuid_5117AAE1116EA8B87A1200060184614--
```

*4.1.3.10 **Batch Results Retrieval Response Message (non-normative)**[77]*

The Batch Results Retrieval Response message structure shown below specifies SOAP 1.2 and MTOM. This shows the following:

---

[76] The Batch Payload retrieval within a Generic Pull interaction (i.e., step 1 in the sequence diagram in §7.3.3.2) uses the same request message as the Batch Results Retrieval Request message structure depicted below, with different *PayloadType* values based on what is being retrieved.

[77] The Batch Payload retrieval within a Generic Pull interaction (i.e., step 1 in the sequence diagram in §7.3.3.2) uses the same request message as the Batch Results Retrieval Request message structure depicted below, with different *PayloadType* values based on what is being retrieved.

1. The HTTP Headers are shown colored in blue.
2. The portion of the SOAP envelope colored in green has the metadata that is defined as part of the Phase IV CAQH CORE Connectivity Rule v4.0.0. (See §4.4)
3. The MTOM Attachment is colored in orange.

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: multipart/related; boundary=MIMEBoundaryurn_uuid_0B72121B1FEFA9BDD31200060195339;
type="application/xop+xml"; start="0.urn:uuid:0B72121B1FEFA9BDD31200060195340@apache.org"; start-
info="application/soap+xml"; action="BatchResultsRetrievalTransaction"

--MIMEBoundaryurn_uuid_0B72121B1FEFA9BDD31200060195339
Content-Type: application/xop+xml; charset=UTF-8; type="application/soap+xml"
Content-Transfer-Encoding: binary
Content-ID: <0.urn:uuid:0B72121B1FEFA9BDD31200060195340@apache.org>

<soapenv:Envelope xmlns:soapenv="http://www.w3.org/2003/05/soap-envelope">
        <soapenv:Body>
              <ns1:COREEnvelopeBatchResultsRetrievalResponse
              xmlns:ns1="http://www.caqh.org/SOAP/WSDL/CORERule4.0.0.xsd">
                    <PayloadType>X12_278_Response_005010X217E1_2</PayloadType>
                    <ProcessingMode>Batch</ProcessingMode>
                    <PayloadID>f81d4fae-7dec-11d0-a765-00a0c91e6bf6</PayloadID>
                    <PayloadLength>1551254</PayloadLength>
                    <TimeStamp>2007-08-30T10:20:34Z</TimeStamp>
                    <SenderID>PayerB</SenderID>
                    <ReceiverID>HospitalA</ReceiverID>
                    <CORERuleVersion>4.0.0</CORERuleVersion>
                    <CheckSum>43B8485AB5</CheckSum>
                   <Payload>
                   <xop:Include href="cid:1.urn:uuid:5117AAE1116EA8B87A1200060184692@apache.org"
                   xmlns:xop="http://www.w3.org/2004/08/xop/include" />
                    </Payload>
                    <ErrorCode>Success</ErrorCode>
                    <ErrorMessage></ErrorMessage>
               </ns1:COREEnvelopeBatchResultsRetrievalResponse>
        </soapenv:Body>
 </soapenv:Envelope>

--MIMEBoundaryurn_uuid_0B72121B1FEFA9BDD31200060195339
Content-Type: image/jpeg
Content-Transfer-Encoding: binary
Content-ID: <1.urn:uuid:5117AAE1116EA8B87A1200060184692@apache.org>

<Response batch file>

--MIMEBoundaryurn_uuid_0B72121B1FEFA9BDD31200060195339--
```

*4.1.3.11 **Batch Results Acknowledgement Submission Message (non-normative)***[78]

The Batch Results Acknowledgement Submission message structure shown below specifies SOAP 1.2, and also uses MTOM (See §7.2) to send the payload file. This shows the following:

1. The HTTP Headers are shown colored in blue.
2. The portion of the SOAP envelope colored in green has the metadata that is defined as part of the Phase IV CAQH CORE Connectivity Rule v4.0.0. (See §4.4)
3. The Batch file (MTOM attachment) is shown colored in orange.

[78] The acknowledgment submission within a Generic Pull interaction (i.e., step 3 in the sequence diagram in §7.3.3.2) uses the same request message as the Batch Results Acknowledgement Submission message structure depicted below, with different *PayloadType* values as appropriate.

```
POST /CORE/PriorAuthBatch HTTP/1.1
Content-Type: multipart/related; boundary=MIMEBoundaryurn_uuid_5117AAE1116EA8B87A1200060184614;
type="application/xop+xml"; start="0.urn:uuid:5117AAE1116EA8B87A1200060184615@apache.org"; start-
info="application/soap+xml"; action="BatchResultsAckTransaction"

--MIMEBoundaryurn_uuid_5117AAE1116EA8B87A1200060184614
Content-Type: application/xop+xml; charset=UTF-8; type="application/soap+xml"
Content-Transfer-Encoding: binary
Content-ID: <0.urn:uuid:5117AAE1116EA8B87A1200060184615@apache.org>

<soapenv:Envelope xmlns:soapenv="http://www.w3.org/2003/05/soap-envelope">
       <soapenv:Body>
              <ns1:COREEnvelopeBatchResultsAckSubmission
              xmlns:ns1="http://www.caqh.org/SOAP/WSDL/CORERule4.0.0.xsd">
                     <PayloadType>X12_999_SubmissionRequest_005010X231A1</PayloadType>
                     <ProcessingMode>Batch</ProcessingMode>
                     <PayloadID>f81d4fae-7dec-11d0-a765-00a0c91e6bf6</PayloadID>
                     <PayloadLength>1551254</PayloadLength>
                     <TimeStamp>2007-08-30T10:20:34Z</TimeStamp>
                     <SenderID>HospitalA</SenderID>
                     <ReceiverID>PayerB</ReceiverID>
                     <CORERuleVersion>4.0.0</CORERuleVersion>
                     <CheckSum>43B8485AB5</CheckSum>
                    <Payload>
                    <xop:Include href="cid:1.urn:uuid:5117AAE1116EA8B87A1200060184692@apache.org"
                    xmlns:xop="http://www.w3.org/2004/08/xop/include" />
                     </Payload>
              </ns1:COREEnvelopeBatchResultsAckSubmission>
       </soapenv:Body>
 </soapenv:Envelope>

--MIMEBoundaryurn_uuid_5117AAE1116EA8B87A1200060184614
Content-Type: image/jpeg
Content-Transfer-Encoding: binary
Content-ID: <1.urn:uuid:5117AAE1116EA8B87A1200060184692@apache.org>

<999 file>

--MIMEBoundaryurn_uuid_5117AAE1116EA8B87A1200060184614--
```

*4.1.3.12 **Batch Results Acknowledgement Submission Response Message (non-normative)***[79]

The Batch Results Acknowledgement Submission Response message structure shown below specifies SOAP 1.2 and MTOM. This shows the following:

1. The HTTP Headers are shown colored in blue.
2. The portion of the SOAP envelope colored in green has the metadata that is defined as part of the Phase IV CAQH CORE Connectivity Rule v4.0.0. (See §4.4)

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: multipart/related; boundary=MIMEBoundaryurn_uuid_0B72121B1FEFA9BDD31200060195339;
type="application/xop+xml"; start="0.urn:uuid:0B72121B1FEFA9BDD31200060195340@apache.org"; start-
info="application/soap+xml"; action="BatchResultsAckTransaction"

--MIMEBoundaryurn_uuid_0B72121B1FEFA9BDD31200060195339
Content-Type: application/xop+xml; charset=UTF-8; type="application/soap+xml"
Content-Transfer-Encoding: binary
Content-ID: <0.urn:uuid:0B72121B1FEFA9BDD31200060195340@apache.org>

<soapenv:Envelope xmlns:soapenv="http://www.w3.org/2003/05/soap-envelope">
        <soapenv:Body>
```

[79] The response to the acknowledgment submission within a Generic Pull interaction (i.e., step 4 in the sequence diagram in §7.3.3.2) uses the same response message as the Batch Results Acknowledgement Submission Response message structure depicted below, with different *PayloadType* values as appropriate.

```
                <ns1:COREEnvelopeBatchResultsAckSubmissionResponse
                xmlns:ns1="http://www.caqh.org/SOAP/WSDL/CORERule4.0.0.xsd">
                        <PayloadType>X12_Response_ConfirmReceiptReceived</PayloadType>
                         <ProcessingMode>Batch</ProcessingMode>
                         <PayloadID>f81d4fae-7dec-11d0-a765-00a0c91e6bf6</PayloadID>
                         <TimeStamp>2007-08-30T10:20:34Z</TimeStamp>
                         <SenderID>PayerB</SenderID>
                         <ReceiverID>HospitalA</ReceiverID>
                         <CORERuleVersion>4.0.0</CORERuleVersion>
                         <ErrorCode>Success</ErrorCode>
                         <ErrorMessage></ErrorMessage>
                 </ns1:COREEnvelopeBatchResultsAckSubmissionResponse>
        </soapenv:Body>
 </soapenv:Envelope>

--MIMEBoundaryurn_uuid_0B72121B1FEFA9BDD31200060195339--
```

*4.1.3.13 **Error Message Structure (non-normative)***

The Error message structure shown below uses the SOAP Fault specifications within SOAP 1.2. As described in §4.2.4, SOAP Faults must be used to send errors at the SOAP level. The HTTP Headers are shown colored in blue. The remainder of the request is the SOAP Envelope.

```
HTTP/1.1 500
Content-Length: 2408
Content-Type: application/soap+xml


<soapenv:Envelope xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/" xmlns: soapenv ="
http://www.w3.org/2003/05/soap-envelope/" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<soapenv:Header>

</soapenv:Header>

<soapenv:Body>

 <soapenv:Fault>
  <soapenv:Code><env:Value>env:Client</env:Value></env:Code>
  <soapenv:Reason>
   <soapenv:Text xml:lang="en">There was an error in the incoming SOAP request</env:Text>
  </soapenv:Reason>
  </soapenv:Fault>
</soapenv:Body>

</soapenv:Envelope>
```

*4.1.3.14 **Envelope Processing Error Message (non-normative)***

The Error message structure shown below illustrates a SOAP-based message that indicates an error has occurred within processing the envelope. The HTTP Headers are shown colored in blue. The remainder of the request is the SOAP Envelope. The envelope structure and metadata that is defined within Phase IV CAQH CORE Connectivity Rule v4.0.0 is colored in green.

```
HTTP/1.1 200 OK
Content-Type: application/soap+xml;
action="http://www.caqh.org/SOAP/WSDL/CORETransactions/RealTimeTransactionResponse";charset=UTF-8

<soapenv:Envelope xmlns:soapenv="http://www.w3.org/2003/05/soap-envelope">
       <soapenv:Body>
              <ns1:COREEnvelopeRealTimeResponse
              xmlns:ns1="http://www.caqh.org/SOAP/WSDL/CORERule4.0.0.xsd">
                      <PayloadType>CoreEnvelopeError</PayloadType>
                      <ProcessingMode>RealTime</ProcessingMode>
                      <PayloadID>f81d4fae-7dec-11d0-a765-00a0c91e6bf6</PayloadID>
                      <TimeStamp>2007-08-30T10:20:34Z</TimeStamp>
                      <SenderID>PayerB</SenderID>
```

```
                        <ReceiverID>HospitalA</ReceiverID>
                        <CORERuleVersion>4.0.0</CORERuleVersion>
                        <Payload></Payload>
            <ErrorCode>VersionMismatch</ErrorCode>
                        <ErrorMessage>Expecting Version X, received Version Y</ErrorMessage>
                </ns1:COREEnvelopeRealTimeResponse>
        </soapenv:Body>
</soapenv:Envelope>
```

4.1.4 Real Time and Batch Payload Attachment Handling

Payload must be sent as an MTOM[80] encapsulated object.

4.2 General Specifications Applicable to the SOAP Envelope Method

4.2.1 Required Transport Method

HIPAA-covered entities or their agents must be able to implement HTTP/S Version 1.1 over the public Internet as a transport method for the third set of the ACA Section 1104 required transactions as specified in §1 of this rule. Receivers (servers) must be able to perform the role of an HTTP/S server, while senders (clients) must be able to perform the role of an HTTP/S client. By using the HTTP/S protocol, all information exchanged between the sender (client) and receiver (server) is encrypted by a session-level private key negotiated at connection time.

4.2.2 Request and Response Handling

HTTP/S supports a request-response message pattern, meaning that the sender (client) submits a message and then waits for a response from the message receiver (server). This works well for the submission of ASC X12N messages in both Batch and Real Time Processing Modes, but the response message from the receiver (server) is different depending on whether the sender's (client's) message is a Real Time request, Batch submission, or Batch request pickup.

4.2.3 Real Time Requests

Real Time requests must include a single inquiry or submission as specified in the transaction's corresponding Phase IV CAQH CORE Infrastructure Rule. In this processing mode the response from the message receiver (server) is either

- A transport or message envelope error response (See §4.2.6)

Or

- The corresponding ASC X12 message response (e.g. ASC X12C 005010X231A1 Implementation Acknowledgement for Health Care Insurance (999) [hereafter ASC X12C v5010 999]

Or

- The corresponding ASC X12N v5010 response transaction to the submitted request

4.2.4 Batch Submission

Batch requests are sent in the same way as Real Time requests. In this Processing Mode the response will differ because message receivers (servers) are not required to provide a corresponding ASC X12 response in the timeframes specified in the transaction's corresponding Phase IV CAQH CORE Infrastructure Rule for Real Time.

For Batch submissions, the response must be only the standard SOAP message indicating whether the request was accepted or rejected. Message receivers (servers) must not respond to a batch submission with an ASC X12

[80] MTOM is defined in Appendix §7.2: *Definitions and Abbreviations used in this Rule.*

response, such as an ASC X12C v5010 999 in the HTTP response to the batch request, even if their systems' capabilities allow such a response. All ASC X12 responses must be available for pick up by the message sender (client) in accordance with the respective Phase IV CAQH CORE Infrastructure Rule for the transaction.

4.2.5 Batch Response Pickup

Batch responses must be picked up after the message receiver (server) has had a chance to process a Batch submission corresponding ASC X12 response in the timeframes specified in the transaction's corresponding Phase IV CAQH CORE Infrastructure Rule.

Under this usage pattern, the message sender (client) connects to the message receiver (server) using HTTP/S and sends a SOAP message requesting available files, and the responder then sends back the file(s) in the HTTP/S SOAP response message (payload).

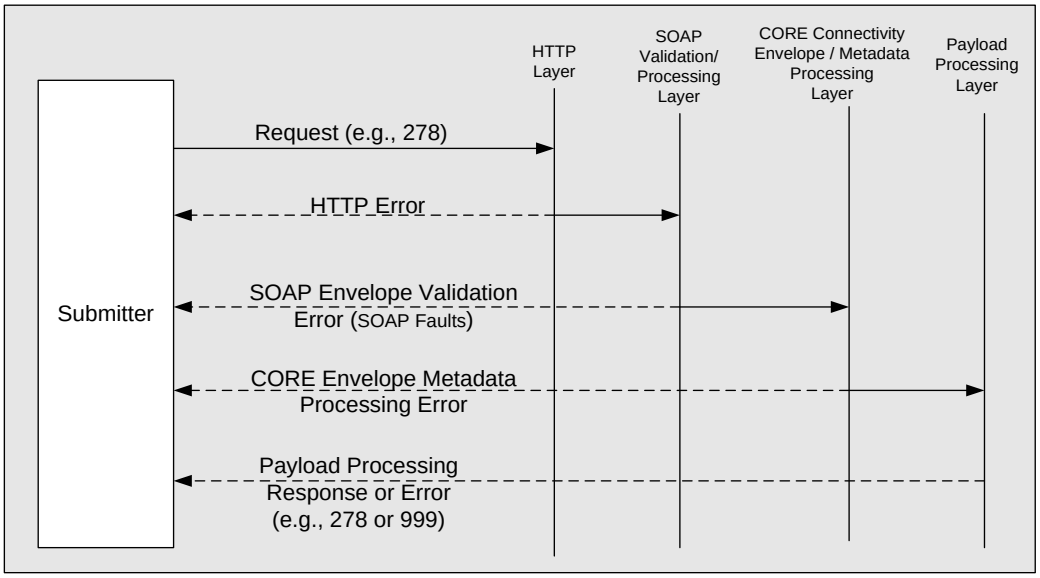
4.2.6 Error Handling

As shown in Figure #4.2.6 below, a submitted request goes through at least four logical layers that process the request. Errors relative to OSI Layers 3 and below are not addressed.

- Processing of HTTP headers (typically handled by a web-server)
- Validating the SOAP Envelope (can be handled by messaging middle-ware or integration brokers)
- Processing the CORE specific metadata located in the SOAP Envelope
- Processing the Payload (e.g., ASC X12, typically handled by application business logic)

Once a request (e.g., ASC X12N v5010 278 Request) is submitted it goes through these four logical layers. At each of these layers, some part of the request is processed. At each layer there can be errors (indicated by the dotted arrows being returned to the request submitter), which may be returned to the request submitter. If there is an error in processing the message at any logical layer, the request does not get passed to the next layer. If no errors are encountered at that layer, the request is passed to the next processing layer. The last logical layer that processes the request is the Payload Processing Layer. Once this layer processes the payload, it returns a response or error (e.g., ASC X12N v5010 278 Response or ASC X12C v5010 999 or ASC X12C TA1).

Figure #4.2.6



Note: In Figure #4.2.6 above, the dotted line arrows indicate error messages being returned to the Submitter if there is a processing error at the corresponding logical processing layer. The straight line arrows indicate the request and response messages.

4.2.6.1 HTTP Status and Error Codes (Normative, Not Comprehensive[81])

The processing and error codes for the HTTP Layer are defined as part of the HTTP specifications [*http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html*]. The intended use of these status and error codes in processing the requests are specified in Table 4.2.6.1 and are consistent with the HTTP status codes from Phase I CAQH CORE.

The status and error codes included in Table 4.2.6.1 only represent a short list of several commonly used status codes in the standard. An exhaustive list of HTTP Status Codes and descriptions are included in the HTTP specification [http://tools.ietf.org/html/rfc2616#section-6.1.1]. This rule requires the use of the appropriate HTTP error or status codes as applicable to the error/status situation. The list of status/error codes below is not intended to constrain the use of standard HTTP status/error codes relative to their original specification. The descriptions below are not intended to override the original definitions but to provide contextual information based on the use of these HTTP Status and Error Codes for CAQH CORE Connectivity error handling.

Table 4.2.6.1

HTTP Status/Error Codes (Normative, Not Comprehensive)	CAQH CORE Rule Specific Description [82] (Intended Use)
200 OK	Success
202 Accepted	Real Time or Batch file submission has been accepted (but not necessarily processed)
400 Bad Request	Incorrectly formatted HTTP headers
403 Forbidden	Access denied
500 Internal Server Error	The web-server encountered a processing error or there was a SOAP fault

[81] An exhaustive list of HTTP Status Codes and definitions are included in section 6.1.1 of the HTTP specification [http://tools.ietf.org/html/rfc2616#section-6.1.1]
[82] Section 6.1.1 of the HTTP specification http://tools.ietf.org/html/rfc2616#section-6.1.1 .

Table 4.2.6.1	
HTTP Status/Error Codes (Normative, Not Comprehensive)	**CAQH CORE Rule Specific Description [82] (Intended Use)**
5xx Server errors	Standard set of server side errors (e.g., 503 Service Unavailable)

4.2.6.2 SOAP Envelope Validation – SOAP Faults (Normative)

Errors at the SOAP Envelope validation layer are returned as SOAP faults [*http://www.w3.org/TR/soap12-part1/#soapfault*]. The full list of enumerated SOAP Faults may be found in the SOAP 1.2 specification. Table 4.2.6.2 provides perspective on two of the errors that are commonly used in relation to the CAQH CORE Rule.

The set of SOAP Faults below is not comprehensive – additional SOAP Faults that comply with the SOAP 1.2 specifications can be used. The descriptions below are not intended to override the original definitions but to provide contextual information based on the use of these SOAP Faults for CAQH CORE Connectivity error handling.

Table 4.2.6.2	
SOAP Faults (Normative; Not Comprehensive)	**CAQH CORE Rule Specific Description (Intended Use)**
Sender	The envelope sent by the sender (client) did not conform to the expected format. In the case of SOAP, this error should be sent as a SOAP fault with "Sender" fault code.
Receiver	The message could not be processed for reasons attributable to the receiver (server) (e.g., upstream process is not reachable). In the case of SOAP, this error should be sent as a SOAP fault with "Receiver" fault code.

4.2.6.3 CAQH CORE Connectivity Envelope Metadata Processing Status and Error Codes (Normative, Comprehensive)

To handle CAQH CORE-compliant envelope processing status and error codes, two fields called *ErrorCode* and *ErrorMessage* are included in the CORE-compliant Envelope. (See §4.4.2) *ErrorMessage* is a free form text field that describes the error (for the purpose of troubleshooting/logging). When an error occurs, *PayloadType* is set to *CoreEnvelopeError*. The set of *ErrorCode*s in this table is normative and comprehensive, which means the use of other error codes is not permitted.

Table 4.2.6.3	
CORE-compliant Envelope Processing Status/Error Codes (Normative, Comprehensive)	**CAQH CORE Status Code Description[83] (Intended Use)**
Success	Envelope was processed successfully.
<FieldName>Illegal	Illegal value provided for <FieldName>. Value provided is not valid based on the metadata constraints defined in the CAQH CORE Connectivity Rule.

[83] An exhaustive list of HTTP Status Codes and definitions are included in section 6.1.1 of the HTTP specification [http://tools.ietf.org/html/rfc2616#section-6.1.1].

Table 4.2.6.3	
CORE-compliant Envelope Processing Status/Error Codes (Normative, Comprehensive)	**CAQH CORE Status Code Description[83] (Intended Use)**
<FieldName>UnSupported	Value is a legal value, but is not supported by the end point receiving the request. Server Connectivity Guide should indicate where to find specific SOAP Operations if multiple URLs are used to support Phase IV CAQH CORE Connectivity.
VersionMismatch	The CAQH CORE Rule Version sent is not valid at the receiver (server).
UnAuthorized	The sender could not be authorized (e.g., using the fields in the metadata, or using the client certificate information).
NotSupported	A request was received at this server with a valid *PayloadType* or *ProcessingMode* but is currently not implemented by this server (e.g., it may be implemented at a different server within this organization)
ChecksumMismatched	The checksum value computed on the recipient did not match the value that was sent in the envelope.

4.2.6.4 Examples of HTTP Status and Error Codes (non-normative)

The following illustrates the status and error codes that may be returned:

- A SOAP request that has illegal HTTP headers gets a response with HTTP Error Code: "400 Bad Request."
- A SOAP request with an unauthenticated submitter's client certificate gets a response with HTTP Error Code: "403 Forbidden."
- A SOAP request with HTTP headers properly formatted but using the wrong SOAP Version (1.1 instead of 1.2) gets HTTP Status 500.

4.2.6.5 Examples of SOAP Faults (non-normative)

The following illustrates some situations where "Sender" SOAP Faults may be returned:

- Invalid version of SOAP (e.g., SOAP 1.1)
- SOAP envelope does not have a SOAP Body
- SOAP Body does not contain the CAQH CORE Connectivity Elements

The following illustrates some situations where "Receiver" SOAP Faults may be returned:

- Failure to connect to a backend system for processing of the message

4.2.6.6 Examples of CAQH CORE Connectivity Envelope Metadata Processing Error Messages (non-normative)

ErrorMessage field is intended to provide a descriptive text of the error message in free form text, to aid in logging and troubleshooting. It is the responsibility of the implementer to keep this message consistent with the semantics of the *ErrorCode*, and not in conflict with it. The *ErrorMessage* must be related to the *ErrorCode* as defined in the table above. The following illustrates *ErrorMessage* fields that may be returned:

- For *ErrorCode=VersionMismatch*, the *ErrorMessage* could be "Expecting CORERuleVersion=X, Received CORERuleVersion=Y"

- For *ErrorCode=SenderIDIllegal*, the *ErrorMessage* could be "SenderID length exceeds maximum allowed length"
- For *ErrorCode=TimeStampIllegal*, the *ErrorMessage* could be "Timestamp is missing the time-zone information"
- For *ErrorCode=CheckSumIllegal*, the *ErrorMessage* could be "Unknown algorithm", or "Unknown encoding type"
- For *ErrorCode=UnAuthorized*, the *ErrorMessage* could be "Unauthorized Sender – please contact XXX to get proper credentials".
- For *ErrorCode=NotSupported*, the *ErrorMessage* could be "The requested PayloadType is supported at a different URL, please review Connectivity Companion Guide"

4.2.7 Audit Handling

Auditing is a local decision by each trading partner. The CAQH CORE recommended best practice is for each trading partner to audit all the envelope metadata and payload for each transaction.

4.2.8 Tracking of Date and Time and Payload ID

In order to comply with the corresponding transaction's Phase IV CAQH CORE Infrastructure Rules message receivers (servers) will be required to track the times of any received inbound messages, and respond with the outbound message for that Payload ID. In addition, as specified in the CAQH CORE Envelope Metadata Table 4.4.2, message senders (clients) must include the date and time the message was sent in the CORE metadata element Time Stamp

4.2.9 Capacity Plan

*4.2.9.1 **Real Time Transactions***

A HIPAA-covered entity or its agent must have a capacity plan such that it can receive and process a large number of single concurrent Real Time transactions via an equivalent number of concurrent connections. These single transactions must be received, processed and the appropriate response provided back to the sender (client) within response time requirements specified in the transaction's corresponding Phase IV CAQH CORE Infrastructure Rule.

Three major factors affect the specific number of Large Volume of Single Real Time Transactions (See §7.2) capable of being transported and processed within a given CAQH CORE response time frame. They are:

1. The amount of message metadata and message encapsulation structure which is required for each transaction;
2. The characteristics of the message handling software and how concise its design and coding are; and,
3. The architecture of the intervening hardware, software and communication platform.

HIPAA-covered entities or their agents must attest that their capacity planning addresses the above three factors that affect large volume single Real Time processing[84]. HIPAA-covered entities or their agents must also attest that they have the ability to track, on a calendar week basis, any change to their agreed upon volume capacity.

[84] See *Appendix 7.2: Abbreviations and Definitions used in this Rule* for a definition of Large Volume of Single Real time Transactions (Synchronous).

In the circumstances where the transaction volume throughput is exceeded by one of the trading partners, the receiving organization may declare a denial of service event and request a temporary waiver of the applicable CAQH CORE response time rule's performance criteria, and/or other appropriate action.

4.2.9.2 Batch Transactions

The HIPAA-covered entity or its agent's messaging system must have the capability to receive and process large Batch transaction files if the entity supports Batch transactions. These transactions must be received, processed and the appropriate response provided back to the sender (client) within the time specified in the applicable CAQH CORE Rule.

Three major factors that affect the specific number of Large Batch payloads capable of being transported and processed within a given time frame are:

1. The availability and use of capabilities in the messaging protocol which support in-line files, file attachments, and automated integrity assurance routines, etc., together with the quality and characteristics of their implementation;
2. The characteristics of the message handling software and its conciseness of design and coding; and,
3. The architecture of the intervening hardware, software and communication platform.

HIPAA-covered entities or their agents must attest that their capacity planning addresses the above three factors that affect large Batch processing. The maximum number of transaction sets to be included in a large Batch file is determined between trading partners.

4.2.10 Real Time Response, Timeout and Retransmission Requirements

Real Time response time must conform to the transaction's corresponding Phase IV CAQH CORE Infrastructure Rule requirements.

- If a Real Time response message is not received within the 60 second response period, the submitter's (client) system should send a duplicate transaction no sooner than 90 seconds after the original attempt was sent.
- If no Real Time response is received after the second attempt, the submitter's (client) system should submit no more than 5 duplicate transactions within the next 15 minutes.
- If additional attempts result in the same timeout termination, the submitter's (client) system must notify the submitter to contact the receiver directly to determine if system availability problems exist or if there are known Internet traffic constraints causing the delay.

4.3 Publication of Entity-Specific Connectivity Companion Document

Servers must publish detailed specifications in a Connectivity Companion Document on the entity's public web site. CAQH CORE recommends specifying the following. This list of recommendations is not intended to be either exhaustive or prohibitive as the specific details of a trading partner relationship are outside the scope of the CAQH CORE rules.

- CAQH CORE Rule Version for Connectivity.
- Details on the message format and the supported transactions (e.g., Real Time, Batch transactions).
- Details about the entity's ASC X12 Interchange; e.g., will an interchange contain multiple functional groups; will the TA1 be in its own interchange without any functional group(s).
- Value of *ReceiverID* for that site.
- Production and Testing URLs for Real Time and Batch transactions.

- Maximum number of Real Time and Batch transactions that can be sent per minute by a single trading partner (client).
- Maximum size of payload for Batch Processing Mode that can be received by a Server.
- Authentication/Authorization policies using X.509 Client Certificates (e.g., how to enroll and obtain a Client Certificate to connect to that receiver (server).
- Information on obtaining the receiver's (server's) Root Certificate Authority and/or Intermediate Certificate Authority public key certificate.
- System Availability as required by the corresponding transaction's Phase IV CAQH CORE Infrastructure Rule.
- Business/Technical points of contact.
- Rules of behavior for programs that connect to this site (e.g., must not deliberately submit Batch files that contain Viruses).
- If the Server only accepts FIPS 140-2 compliant connections, or if the Server organization security policy requires a stronger transport security than SSL v3.0, the version of TLS (1.1 or higher), and the algorithm (e.g., SHA-2) that is expected for Checksum element.

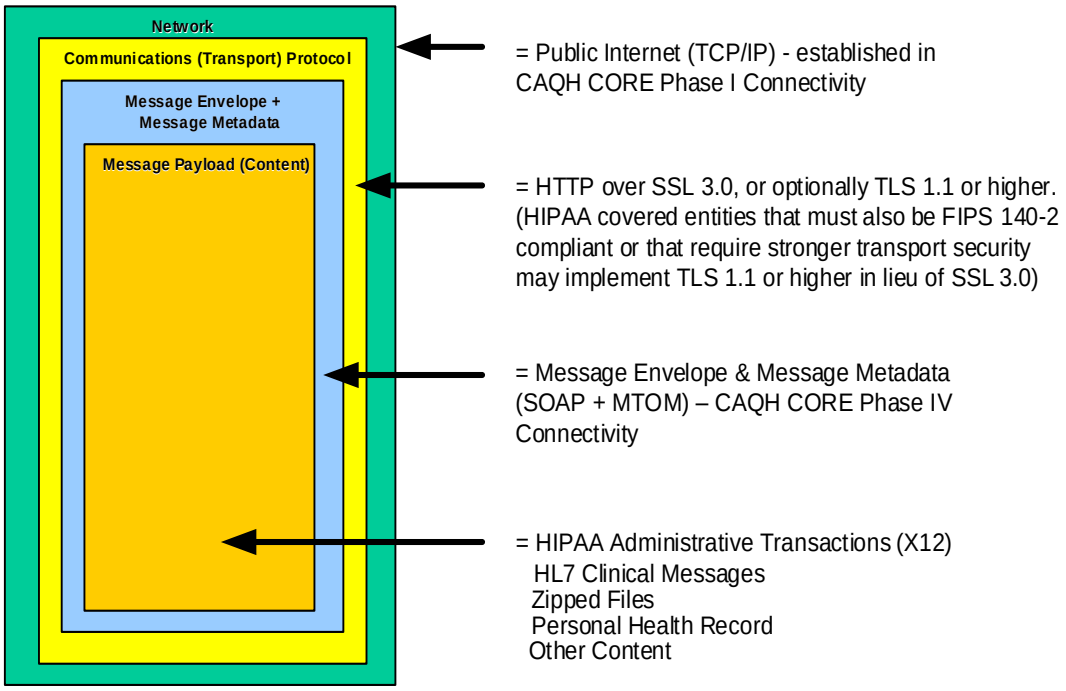
4.4 Envelope Metadata Fields, Descriptions, Intended Use and Syntax/Value-Sets

The Envelope Metadata specified in Table 4.4.2 below pertains to the Phase IV Message Envelope SOAP+WSDL. With the exception of *ErrorCode* and *ErrorMessage* fields, which are only sent in the response, the Phase IV CAQH CORE required envelope metadata for the request and response are required to be identical.

4.4.1 Message Envelope

As shown in Figure #4.4.1 below, the Message Envelope is outside the Message Payload (content), and inside the transport protocol envelope. The Phase I CAQH CORE 153 Connectivity Rule v1.1.0 established the use of HTTP/S as the transport protocol over the public Internet, hence the transport protocol envelope consists of HTTP headers. Examples of message payload include HIPAA administrative transactions (ASC X12), HL7 clinical messages, zipped files, etc.

Figure 4.4.1



4.4.2 Table of CAQH CORE Envelope Metadata

Table 4.4.2 CAQH CORE Envelope Metadata

Non-normative (Descriptive)			Normative (Definitive)			
Element	**Description**	**Expected Use**	**Field Name[85]**	**Requirement Indicator for Real Time and Batch**	**DataType**	**Field Constraints or Value-sets (Not Comprehensive)**
Payload Type	Payload Type specifies the type of payload included within a request, (e.g. HIPAA ASC X12N transaction set 837, 820, 278, etc.).	• Message routing • Efficient processing • Auditing	PayloadType	Required for both	Coded Set	Please see Phase IV CAQH CORE-required Payload Type Table document for enumeration of PayloadType field.
Processing Mode	Processing Mode indicates Batch or Real Time[86] Processing Mode (as defined by CORE)	• Messaging routing • Resource allocation • Transaction scheduling • Message or transaction auditing	ProcessingMode	Required for both	Coded Set	RealTime, Batch

[85] Mixed case or Camel Case (e.g., *PayloadType*) capitalization is used for the field names to provide readability within the messages http://en.wikipedia.org/wiki/CamelCase.
[86] See *Appendix 7.2: Abbreviations and Definitions used in this Rule* for a definition of Batch and Real Time.

Table 4.4.2 CAQH CORE Envelope Metadata						
Non-normative (Descriptive)			**Normative (Definitive)**			
Element	**Description**	**Expected Use**	**Field Name[85]**	**Requirement Indicator for Real Time and Batch**	**DataType**	**Field Constraints or Value-sets (Not Comprehensive)**
Payload Length	Defines the length of the actual payload in bytes.	• Efficient processing and resource allocation. • Auditing • Trouble-shooting	PayloadLength	Required for Batch interactions except under certain conditions[87] Shall not be used for Real time.	Integer (Base 10)	
Payload ID	Payload ID (unique within the domain of the party that sets this value) is a payload identifier assigned by the Sender in both Batch and Real Time Processing Modes. If the payload is being resent in the absence of confirmation of receipt to persistent storage, the same PayloadID may be re-used.	• Auditing • Trouble-shooting	PayloadID	Required for both Real Time and Batch.	String	*PayloadID* will conform to ISO UUID standards (described at ftp://ftp.rfc-editor.org/in-notes/rfc4122.txt), with hexadecimal notation, generated using a combination of local timestamp (in milliseconds) as well as the hardware (MAC) address[88], to ensure uniqueness.
Time Stamp	The Sender (request) or Receiver (response) Time Stamp. This does not require a shared time server for consistent time.	• Auditing • Trouble-shooting	TimeStamp	Required for both	dateTime	dateTime (http://www.w3.org/TR/xmlschema11-2/#dateTime)

[87] Some requests or responses within Batch interactions may not have a payload. This could occur when requesting a payload or when there is no payload in the response.
[88] In multithreaded environments, in addition to the hardware (MAC) address and timestamp, the Process-ID or Thread-ID may also be used as additional parameters to ensure *PayloadID* uniqueness across multiple processes and/or threads. However, the use of MAC address is not a requirement of this rule.

Table 4.4.2 CAQH CORE Envelope Metadata						
Non-normative (Descriptive)			**Normative (Definitive)**			
Element	**Description**	**Expected Use**	**Field Name[85]**	**Requirement Indicator for Real Time and Batch**	**DataType**	**Field Constraints or Value-sets (Not Comprehensive)**
Sender Identifier	A unique[89] business entity identifier representing the message envelope creator. Sender Identifier is better suited for identifying business entities and trading partners than User Name because: • User Name is usually anonymized for security reasons and to protect privacy. • User Name attribute does not exist if another authentication method is used. • Authentication and messaging may happen on different layers[90] and therefore may be handled by disparate applications and processes.	• Message routing and processing by a receiver • Transaction auditing. • As a reference to a business agreement.	SenderID	Required	String	Maximum length 50 characters The use of OIDs (e.g., HL7 or IANA) is recommended, but not required.
Receiver Identifier	A unique[91] business entity identifier representing the next-hop receiver.	• Transaction auditing. • As a reference to a business agreement. • Message routing by the receiver.	ReceiverID	Required	String	Maximum length 50 characters The use of OIDs (e.g., HL7 or IANA) is recommended, but not required.
CORE Rule Version	The CORE Rule version that this envelope is using. For response messages returned by a Server, this is the version of the Server implementation.	• Message routing and processing. • Auditing	CORERuleVersion	Required for both	Coded Set	4.0.0

[89] Unique within the Sender's (client's) domain.
[90] §2 shows the layers in the OSI model.
[91] Unique within a Receiver's (server's) domain.

Table 4.4.2 CAQH CORE Envelope Metadata						
Non-normative (Descriptive)			**Normative (Definitive)**			
Element	**Description**	**Expected Use**	**Field Name[85]**	**Requirement Indicator for Real Time and Batch**	**DataType**	**Field Constraints or Value-sets (Not Comprehensive)**
Checksum	An element used to allow receiving site to verify the integrity of the message that is sent.	Message Integrity verification	CheckSum	Required for Batch interactions except under certain conditions[92] Not used for Real Time	String	Algorithm is SHA-1[93] Encoding is Hex. Checksum must be computed only on the payload and not on the metadata.
Error Code	Error code to indicate the error when processing the envelope.	• Error handling • Troubleshooting	ErrorCode	Required in Response (for both Real Time and Batch) Not used in Request.	Coded Set	Please see Section on Error Handling for a definition of error codes.
Error Message	Text Error message that describes the condition that caused the error. The text of the *ErrorMessage* must provide additional information describing how the Error can be resolved, and must not provide conflicting information from that provided in the *ErrorCode.*	• Logging • Troubleshooting	ErrorMessage	Required in Response (for both Real Time and Batch) Not used in Request	String	Maximum length of 1024 characters. Please see Section on Error Handling for examples of Error Messages.

4.4.3 Specification of Processing Mode and Enumeration Payload Type Fields

4.4.3.1 ***Processing Mode Table (Normative)***

A HIPAA-covered entity or its agent must support the transaction processing mode requirements (i.e., Real Time and/or Batch) as specified in the *COREProcessingModePayloadTypeTables.docx* companion document to this Phase IV CAQH CORE 470 Connectivity Rule v4.0.0 when exchanging transactions in conformance with this Phase IV CAQH CORE 470 Connectivity Rule v4.0.0.

The Processing Mode requirements specified in the Phase IV CAQH CORE-required Processing Mode Table also apply when a HIPAA-covered entity or its agent are exchanging the transactions addressed by this rule using any other connectivity method as permitted by the CAQH CORE Safe Harbor. (See §5.)

[92] Some requests or responses within Batch interactions may not have a payload. This could occur when requesting a payload or when there is no payload in the response.
[93] Entities requiring FIPS 140-2 compliance may use SHA-2 instead of SHA-1. If SHA-2 is used, then the entity's Connectivity Companion Document will specify that SHA-2 is expected in incoming messages from trading partners.

*4.4.3.2 **Enumeration of Payload Types When Handling ASC X12 Payloads (Normative)***

A HIPAA-covered entity or its agent must support the requirements for identifying the payload (*PayloadType)*, which is the essential data being carried within the content of the Message Envelope as specified in the *COREProcessingModePayloadTypeTables.docx* companion document to this Phase IV CAQH CORE Connectivity Rule v4.0.0. (See Figure #4.4.1, Table 4.4.2, and §6.1.). (See §3.7.3 for maintenance requirements.)

*4.4.3.3 **Enumeration Convention for PayloadType when Handling Non-ASC X12 Payloads (Non-normative)***

The Envelope metadata specification in §4.4.3 includes a PayloadType field that is enumerated for ASC X12 payload types. This envelope may also be used to transport other types of payloads. In such cases, the convention for the *PayloadType* field is as follows:

<SDO>_<PayloadType>_<Version>_<Sub-version>

Note: SDO stands for Standards Development Organization.

For example, an HL7 based ADT04 Version 2.3.1 payload may specify the *PayloadType* as *HL7_ADT04_2_3_1*.

5 CAQH CORE Safe Harbor

This rule specifies a "Safe Harbor" that any stakeholder can be assured will be supported by any HIPAA-covered entity or its agent. This rule further specifies the connectivity method that all HIPAA-covered entities or their agents and all voluntarily CORE-certified organizations must implement and with which conformance must be demonstrated.

As such, this rule:

- **DOES NOT** require trading partners (e.g., a provider or a health plan) to discontinue using existing connections that do not match the rule.
- **DOES NOT** require trading partners to use a CAQH CORE-compliant method for all new connections.
- **DOES NOT** require all trading partners to use only one method for any connections.
- **DOES NOT** require any entity to do business with any trading partner or other entity.

CAQH CORE expects that in some circumstances, trading partners may agree to use different communication method(s) and/or security requirements than those described in this rule to achieve the technical goals of the specific connection. Examples of potential different communication methods that could be implemented under this CAQH CORE Safe Harbor provision include a VPN (virtual private network) or SFTP (secure file transfer protocol.) Such connectivity gateways are not considered compliant with this Phase IV CAQH CORE 470 Connectivity Rule v4.0.0. When a HIPAA-covered entity or its agent implement a different communication method(s) as permitted by this CAQH CORE Safe Harbor all payload processing modes specified for the transactions addressed by this rule must be supported in each connectivity gateway implemented which does not comply with this Phase IV CAQH CORE 470 Connectivity Rule v4.0.0 requirements. (See §4.4.3.1)

This Phase IV CAQH CORE 470 Connectivity Rule v4.0.0 is the CAQH CORE Safe Harbor connectivity method that a HIPAA-covered entity or its agent MUST use if requested by a trading partner. If the HIPAA-covered entity or its agent do not believe that this CAQH CORE Safe Harbor is the best connectivity method for that particular trading partner, it may work with its trading partner to implement a different, mutually agreeable connectivity method. However, if the trading partner insists on using this CAQH CORE Safe Harbor, the HIPAA-covered entity or its agent must accommodate that request. This clarification is not intended in any way to modify entities' obligations to exchange electronic transactions as specified by HIPAA or other federal and state regulations.

6 Conformance Requirements

Conformance with this CAQH CORE Operating Rule can be voluntarily demonstrated and certified through successful completion of the approved Phase IV CAQH CORE Voluntary Certification Test Suite with a third party CAQH CORE-authorized Testing Vendor, followed by the entity's successful application for a CORE Certification. A CORE Certification demonstrates that a HIPAA-covered entity has successfully tested for conformity with all of the Phase IV CAQH CORE Operating Rules, and the entity or its product has fulfilled all relevant conformance requirements.

Only the Department of Health and Human Services (HHS) can decide whether a particular entity's system is **compliant** or **noncompliant** with HIPAA Administrative Simplification requirements (which include HIPAA-adopted CAQH CORE Operating Rules). HHS may adjudicate on an entity's compliance and assess civil money penalties or penalty fees for noncompliance under the following HIPAA Administrative Simplification mandates:

- HIPAA regulations mandate that the Secretary "will impose a civil money penalty upon a covered entity or business associate if the Secretary determines that the covered entity or business associate has violated an administrative simplification provision." (47 CFR 160.402)
- Under the ACA, HIPAA mandates a certification process for HIPAA-covered health plans only, under which HIPAA-covered health plans are required to file a statement with HHS certifying that their data and information systems are in compliance with applicable standards and associated operating rules. (Social Security Act, Title XI, Section 1173(h)). HIPAA also mandates that a HIPAA-covered health plan must "ensure that any entities that provide services pursuant to a contact with such health plan shall comply with any applicable certification and compliance requirements"(Social Security Act, Title XI, Section 1173(h)(3)).
- HIPAA also mandates that HHS is to "conduct periodic audits to ensure that health plans… are in compliance with any standards and operating rules." (Social Security Act, Title XI, Section 1173(h))

7 Appendix

7.1 References

Note: These were used for rule creation as well as to create the analysis artifacts as part of Phase IV CAQH CORE Connectivity.

Table 7.1

Author	Document Name	Location
CORE	Claim Status Rule Test Scenario	CORE Operating Rule 250
HL7 (Health Level 7)	HL7 Object Identifier (OID) Registry	http://www.hl7.org/oid/index.cfm
Internet Assigned Numbers Authority (IANA)	IANA Private Enterprise Number (PEN) aka "OID" Registration Page	http://www.iana.org/cgi-bin/enterprise.pl
Internet Engineering Task Force (IETF)	Key Words for use in RFCs to Indicate Requirement Levels	http://www.ietf.org/rfc/rfc2119.txt
Internet Engineering Task Force (IETF)	Uniform Resource Identifier (URI): Generic Syntax	https://www.ietf.org/rfc/rfc3986.txt
Internet Engineering Task Force (IETF)	Hypertext Transfer Protocol – HTTP 1.1	http://tools.ietf.org/html/rfc2616.txt
Internet Engineering Task Force (IETF)	HTTP Authentication: Basic and Digest Access Authentication	http://tools.ietf.org/html/rfc2617.txt
Internet Engineering Task Force (IETF)	The MIME Multipart/Form-Data (RFC 2388)	http://www.ietf.org/rfc/rfc2388.txt
Internet Engineering Task Force (IETF)	TLS 1.1 Specification	http://tools.ietf.org/html/rfc4346.txt
Internet Engineering Task Force (IETF)	Universally Unique IDentifier (UUID) URN Namespace	ftp://ftp.rfc-editor.org/in-notes/rfc4122.txt
NIST 800-52r1	Guidelines for the Selection, Configuration and Use of Transport Layer Security (TLS) Implementations	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf
OASIS	Web Services Reliable Messaging Protocol 1.1 (WS-RM)	http://docs.oasis-open.org/ws-rx/wsrm/v1.1/wsrm.html
OASIS	Web Service Security Core Specification 1.1	http://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf

Table 7.1		
Author	**Document Name**	**Location**
OASIS	Web Service Security SOAP Message Security 1.1	http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-errata-os-SOAPMessageSecurity.pdf
OASIS	Web Service Secure Conversation 1.3	http://docs.oasis-open.org/ws-sx/ws-secureconversation/200512/ws-secureconversation-1.3-os.html
OASIS	Universal Description, Discovery and Integration (UDDI) 1.0	http://www.oasis-open.org/committees/uddi-spec/doc/contribs.htm#uddiv1
OASIS	ebXML Message Service Specification v2.0	http://www.oasis-open.org/committees/ebxml-msg/documents/ebMS_v2_0.pdf
W3C (World Wide Web Consortium)	Extensible Mark-up Language (XML) 1.0 (Fourth Edition)	http://www.w3.org/TR/2006/REC-xml-20060816/
W3C (World Wide Web Consortium)	Namespaces in XML 1.0 (Second Edition)	http://www.w3.org/TR/2006/REC-xml-names-20060816
W3C (World Wide Web Consortium)	Canonical XML Version 1.0	http://www.w3.org/TR/2002/REC-xmldsig-core-20020212
W3C (World Wide Web Consortium)	XML Schema Part 1: Structures Second Edition	http://www.w3.org/TR/2004/REC-xmlschema-1-20041028
W3C (World Wide Web Consortium)	XML Schema Part 2: Datatypes Second Edition	http://www.w3.org/TR/2004/REC-xmlschema-2-20041028
W3C (World Wide Web Consortium)	XML Signature Syntax and Processing	http://www.w3.org/TR/2002/REC-xmldsig-core-20020212
W3C (World Wide Web Consortium)	XML Encryption Syntax and processing	http://www.w3.org/TR/2002/REC-xmlenc-core-20021210
W3C (World Wide Web Consortium)	Simple Object Access Protocol (SOAP) 1.2	http://www.w3.org/TR/soap12-part1/
W3C (World Wide Web Consortium)	SOAP Message Transmission Optimization Mechanism (MTOM)	http://www.w3.org/TR/2005/REC-soap12-mtom-20050125
W3C (World Wide Web Consortium)	Web Services Description Language (WSDL) 1.1	http://www.w3.org/TR/2001/NOTE-wsdl-20010315

7.2 Abbreviations and Definitions Used in this Rule

Table 7.2	
Term or Concept	**Definition**
ASC X12 Interchange	An ASC X12 Interchange is a graphic character string structured using delimited, tagged data concepts. An ASC X12 Interchange begins with an Interchange Control Header segment: Segment ID = ISA and ends with an Interchange Control Trailer segment: Segment ID – IEA. An ASC X12 Interchange may be composed of one or more Functional Groups (GS/GE Control Segments). An ASC X12 Functional Group is composed of one or more Transaction Sets (ST/SE Control Segments). An ASC X12 Interchange may be a Logical file or a physical file as determined by the originator of the Interchange. As such, a physical file may consist of one or more ASC X12 Interchanges. The ISA Interchange Control Header segment does not identify the content of any included Functional Groups. The Functional Group Control Header segment identifies the transaction set(s) in the Functional Group: GS08-480 Version/Release/Industry Indicator Code.
Asynchronous	A message exchange interaction is said to be asynchronous when the associated messages are chronologically and procedurally decoupled, e.g., in a request-response interaction, the client agent can process the response at some indeterminate point in the future when its existence is discovered. Mechanisms to do this include polling, notification by receipt of another message, etc. [WS Glossary, 2004]
Batch (Batch Mode, Batch Processing Mode)	Batch Mode is when the initial (first)[94] communications session is established and maintained open and active only for the time required to transfer a batch file of one or more transactions. A separate (second) communications session is later established and maintained open and active for the time required to acknowledge that the initial file was successfully received and/or to retrieve transaction responses. Batch Processing Mode[95] is also considered to be an asynchronous processing mode, whereby the associated messages are chronologically and procedurally decoupled. In a request-response interaction, the client agent can process the response at some indeterminate point in the future when its existence is discovered. Mechanisms to implement this capability may include: polling; notification by receipt of another message; or receipt of related responses (as when the request receiver "pushes" the corresponding responses back to the requestor), etc. Batch (asynchronous) Processing Mode is from the perspective of both the requester and responder. If a Batch (asynchronous) request is sent via intermediaries, then such intermediaries may, or may not, use Batch Processing Mode to further process the request.
Batch Files (Payload)	A single submission of a message payload that contains one ASC X12 Interchange containing one Functional Group containing one ASC X12 transaction set consisting of more than one business transaction.
Client	An entity that sends/relays a message to a Server.

[94] CORE Phase I Glossary Definitions. http://www.caqh.org/sites/default/files/core/phase-i/reference/PIGlossary.pdf
[95] Ibid.

Table 7.2	
Term or Concept	**Definition**
CAQH CORE Safe Harbor	The connectivity requirements that application vendors, providers, and health plans (or other information sources) are required to support in order to provide assurance that these requirements are supported by any HIPAA-covered entities or their agents.
Extensibility	Extensibility is a property of a system, format, or standard that allows evolution in performance or format within a common framework, while retaining partial or complete compatibility among systems that belong to the common framework.[96] Extensibility is a system design principle where the implementation takes into consideration future growth. It is a systematic measure of the ability to extend a system and the level of effort required to implement the extension. Extensions can be through the addition of new functionality or through modification of existing functionality. The central theme is to provide for change while minimizing the impact to existing system functions.[97]
Federal Information Processing Standards Security Requirements for Cryptographic Modules (FIPS 140-2)	The Federal Information Processing Standards Publication Series of the National Institute of Standards and Technology (NIST) is the official series of publications relating to standards and guidelines adopted and promulgated under the provisions of Section 5131 of the Information Technology Management Reform Act of 1996 (Public Law 104-106) and the Computer Security Act of 1987 (Public Law 100-235). These mandates have given the Secretary of Commerce and NIST important responsibilities for improving the utilization and management of computer and related telecommunications systems in the Federal government. The NIST, through its Information Technology Laboratory, provides leadership, technical guidance, and coordination of government efforts in the development of standards and guidelines in these areas (http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf).
HTTP	Hypertext Transport Protocol Version 1.1 (IETF RFC 2616: http://www.ietf.org/rfc/rfc2616.txt).

[96] http://www.atis.org/glossary/definition.aspx?id=7853 ATIS (Alliance for Telecommunications Industry Solutions http://www.atis.org/about/index.asp.
[97] http://en.wikipedia.org/wiki/Extensibility.

Table 7.2	
Term or Concept	**Definition**
Interoperability	Interoperability is the capability of different information technology systems, software applications and networks to communicate, execute programs, exchange data accurately, effectively and consistently, among various functional units in a manner that requires the user to have little or no knowledge of the unique characteristics of those units and to use the information that has been exchanged.[98] Interoperability also requires no specific architecture and is independent of vendors and their various operating systems, programming languages, hardware, and network infrastructure**.** Functional interoperability is the capability to reliably exchange information without errors. Semantic interoperability allows systems to interpret and make effective use of the information exchanged among systems[99].

[98] Adapted from http://engineers.ihs.com/document/abstract/AQSBFBAAAAAAAAAAA ANSI Information Technology – Vocabulary – Part 1: Fundamental Terms.
[99] HIMSS Position Statement: Adoption of HITSP Interoperability Specifications July 2007.

Table 7.2	
Term or Concept	**Definition**
Interoperability Specification[100]	An Interoperability Specification focuses on a set of constrained standards for information interchange that address the core requirements of the Use Cases. It does not define all functions, constructs and standards necessary to implement a conforming system in the real world environment. An Interoperability Specification defines how two or more systems exchange standard data content in a standard manner. Interoperability Specifications define the necessary business and technical actors, the transactions between them including the message, content and terminology standards for the actual information exchange. Interoperability Specifications do not specify the functional requirements or behaviors of the systems or applications. Interoperability Specifications, unless otherwise noted, are not intended to define or prescribe any system architecture or implementation. At the most basic level, the Interoperability Specifications define specific information exchange standards that are to be used by any two systems. Information exchange must be placed within the context of a transaction between defined technical actors which fulfill higher level business requirements derived from the use cases. In some cases the necessary technical actors may require some architectural structure or make some assumptions involving synchronous or asynchronous data exchanges, or require specific type of exchange, such as a message or document. These requirements may constrain to some degree the total range of choices regarding system architectures. When constraints are necessary to meet the use case requirements, the Interoperability Specification will note this and will retain as much architectural neutrality as possible. When appropriate, Interoperability Specifications may provide architectural examples and discuss considerations of such examples. HITSP and ONC do not define "Interoperability," but, do define "Interoperability Specification."
Large Batch Files (Payload)	A single submission of a message payload that contains more than one ASC X12 Interchange, each of which may contain one or more Functional Groups, each of which may contain one or more ASC X12 transaction sets.
Large Volume of Single Real time Transactions (Synchronous)	A high number of Real Time transactions arriving at the receiving system concurrently. CORE defines large volume as "X"% of an organization's average daily received transaction volume (based on all trading partners) within one minute. "X" is defined by organization.
Media Access Control (MAC) Address	A media access control address (MAC address) is a unique identifier assigned to network interfaces for communications on the physical network segment.
Message Encapsulation Layer	This refers to the Open Systems Interconnect (OSI) layers 5 and 6.

[100] HITSP Interoperability Specification: EHR Lab Terminology Component HITSP/ISC-35 October 20, 2006 Version 1.2.

Table 7.2	
Term or Concept	**Definition**
Message Envelope Standard	SOAP+WSDL, described in Section "Specifications for SOAP + WSDL".
Metadata	Data about data. In the context of CORE Connectivity, metadata is the information in the message envelope that describes the payload.
MTOM	W3C Message Transmission Optimization Mechanism (http://www.w3.org/TR/soap12-mtom/).
Normative	In standards terminology, "normative" means "considered to be a prescriptive part of the standard" [Wikipedia].
Non-normative	Informational, not intended to be part of the specification.
OSI	Open Systems Interconnection Basic Reference Model (OSI Reference Model, or OSI Model for short) is a layered, abstract description for communications and computer network protocol design. From top to bottom, the OSI Model consists of the Application, Presentation, Session, Transport, Network, Data Link and Physical Layers [Wikipedia].
Open Standard [101]	"Open Standards" are those standards made available to the general public and are developed (or approved) and maintained via a collaborative and consensus driven process. Open Standards facilitate interoperability and data exchange among different products or services and are intended for widespread adoption.
Payload	The essential data that is being carried within a packet or other transmission unit. The payload does not include the "overhead" data required to get the packet to its destination. A packet is the unit of data that is routed between an origin and a destination on the Internet or any other packet-switched network. When any file (e-mail message, HTML file, Graphics Interchange Format file, Uniform Resource Locator request, and so forth) is sent from one place to another on the Internet, the Transmission Control Protocol (TCP) layer of TCP/IP divides the file into "chunks" of an efficient size for routing. Each of these packets is separately numbered and includes the Internet address of the destination. The individual packets for a given file may travel different routes through the Internet. When they have all arrived, they are reassembled into the original file (by the TCP layer at the receiving end).[102]

[101] International Telecommunication Union – Open Standards Definition. http://www.itu.int/ITU-T/othergroups/ipr-adhoc/openstandards.html.
[102] SearchSecurity.com. http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci214475,00.html.

Table 7.2	
Term or Concept	**Definition**
Performance	According to the Phase I CAQH CORE 153 Connectivity Rule, performance is defined in only two components: Response Time – the time required to receive a Request, process it completely and send an appropriate response, as specified in the Phase I CAQH CORE Eligibility and Benefits Rules and Policies for Real time [103] and Batch [104] exchanges. System Availability – the time an information source's (health plan, clearinghouse/switch or other intermediary system) processing system is capable of properly processing Request/Response transactions, as specified in the Phase I CAQH CORE Eligibility and Benefits Rules and Policies for system availability [105].

[103] CORE Phase I 156: Eligibility and Benefits Real Time Response Time Rule
[104] CORE Phase I 155: Eligibility and Benefits Batch Response Time Rule
[105] CORE Phase I 157: Eligibility and Benefits System Availability

Table 7.2	
Term or Concept	**Definition**
Performance Evaluation Criteria	For the purpose of evaluating the measurable performance dimensions of potential messaging methodologies to be used in Real time healthcare transactions, Performance Evaluation Criteria may include: Response Time – the time required to receive a Request, process it completely, and send an appropriate response.[106] Maximum Arrival Rate Before Saturation – the maximum number of properly formed arriving Request transactions per time period (usually seconds or minutes), above which the ability for increased acceptance for further processing stops.[107] Overhead Information – Digital information transferred across the functional interface between a user and a telecommunications system, or between functional units within a telecommunications system, for the purpose of directing or controlling the transfer of user information or the detection and correction of errors. Note: Overhead information originated by the user is not considered to be system overhead information. Overhead information generated within the communications system and not delivered to the user is system overhead information. Thus, the user throughput is reduced by both overheads while system throughput is reduced only by system overhead.[108] Capacity – the maximum number of completed Request/ Response transaction sets per specific time period. Quality of Service – the number of properly and accurately completed Request/Response transaction sets divided by the number of properly submitted transactions (Requests). When making such performance measurements and evaluations, it is important to consider the architecture of networks and systems to assure their similarity, and/or to assess the relevance and impact of any differences.
Processing Mode	Processing modes or computing modes are classifications of different types of computer processing, e.g., batch, real time. In the context of CAQH CORE Operating Rules, the concept of processing mode applies to the timeframe within which a receiver of a payload of transactions processes those transactions and returns to the sender of the payload appropriate acknowledgements. See Batch and Real Time for CAQH CORE definitions.

[106] CORE Phase I 156: Eligibility and Benefits Real Time Response Time Rule; and CORE Phase I 155: Eligibility and Benefits Batch Response Time Rule.
[107] http://www.cs.washington.edu/homes/lazowska/qsp/Contents.pdf Quantitative System Performance, Chapter 5.2.1. Transaction Workloads (Page 72).
[108] http://www.atis.org/tg2k/ and search "Overhead Information" ATIS (Alliance for Telecommunications Industry Solutions http://www.atis.org/about/index.asp.

Table 7.2	
Term or Concept	**Definition**
Real time (Real time Mode, Real time Processing Mode) [109]	Real Time Mode [110] is when an entity is required to send a transaction and receive a related response within a single communications session, which is established and maintained open and active until the required response is received by the entity initiating that session. Communication is complete when the session is closed. Real Time Mode & Real Time Processing Mode are also considered to be a synchronous processing mode. (See Synchronous). Real Time, or synchronous, Processing Mode is from the perspective of both the requester and responder.
Safe Harbor	A "Safe Harbor" is generally defined as a statutory or regulatory provision that provides protection from a penalty or liability.[111] In many IT-related initiatives, a safe harbor describes a set of standards/guidelines that allow for an "adequate" level of assurance when business partners are transacting business electronically.
Secure Sockets Layer (SSL)	See Transport Layer Security.
Server	An entity that receives a message from a Client, which it may process, or relay to another Server.
SOAP	W3C Simple Object Access Protocol Version 1.2. (http://www.w3.org/TR/soap12-part1/)
Standard	A standard is a document, established by consensus and approved by a recognized body that provides, for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context.[112]
Standard Development Organization	Standards Development Organizations (SDOs) are organizations whose processes are accredited by ANSI. A SDO may also include non-ANSI accredited organizations such as W3C, OASIS, ISO, UN/CEFACT and IETF.
Support [Supported]	Means that the entity must have the capability as specified and required.
Submitter Authentication	X.509 Certificate based Authentication over SSL or TLS, described in Sub-section "Submitter Authentication Handling."
Synchronous	The application sending the request message waits for the response, which is returned on the same communications connection (i.e., synchronous request/reply). This message exchange pattern is used for most real time transactions.

[109] CORE Phase I Glossary Definitions. http://www.caqh.org/sites/default/files/core/phase-i/reference/PIGlossary.pdf
[110] Ibid.
[111] Merriam-Webster's Dictionary of Law. Merriam-Webster, Inc., 28 May, 2007. <Dictionary.com http://dictionary.reference.com/browse/safeharbor>.
[112] http://isotc.iso.org/livelink/livelink/fetch/2000/2122/830949/3934883/3935096/07_gen_info/faq.html.

Table 7.2	
Term or Concept	**Definition**
Transport Layer Security (TLS)	Transport Layer Security (TLS)[113] and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols that "provide communications security over the Internet". TLS and SSL encrypt the segments of network connections above the Transport Layer, using symmetric cryptography for privacy and a keyed message authentication code for message reliability. Several versions of the protocols are in widespread use in applications like web browsing, electronic mail, Internet faxing, instant messaging and voice-over-IP (VoIP). TLS is an IETF standards track protocol, last updated in RFC 5246, and is based on the earlier SSL specifications developed by Netscape Corporation (http://tools.ietf.org/html/rfc5246). Future enhancements and development by the IETF will occur within the TLS specification.
WSDL	W3C Web Services Definition Language Version 1.1 (http://www.w3.org/TR/2001/NOTE-wsdl-20010315).

7.3 Sequence Diagrams

The UML sequence diagrams below show interactions between a client and a server. When the interactions include multiple requests/responses, each pair of requests and its corresponding (synchronous) response is shown encapsulated in a white rectangle. Each request followed by synchronous response (shown in a single white rectangle) is in a client-server connection that can be expected to be opened for a request and closed after the corresponding synchronous response is received. Subsequent requests/responses occur in new client-server connections. Servers are stateless and are not assumed to keep session information between connections, unless such information is sent as part of the requests (e.g., using ASC X12C 999 or ASC X12C TA1 payloads).

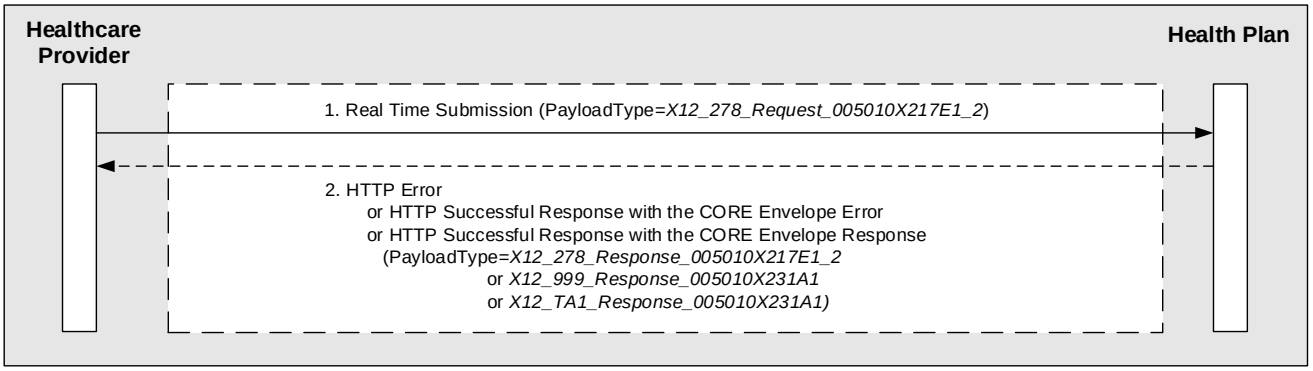
7.3.1 Real Time Interaction

This section describes Real Time interactions that include the following steps:

- Submission of Real Time Payload (step 1 in the diagrams)
- Real Time (Synchronous) response (step 2 in the diagrams)

Example 1: Health Care Services Review – Request for Review and Response (ASC X12N v5010 278)

The UML sequence diagram below shows a *Health Care Services Review – Request for Review and Response* Real Time transaction between a HIPAA-covered Healthcare Provider and a HIPAA-covered Health Plan. The interactions are described in the diagram below.



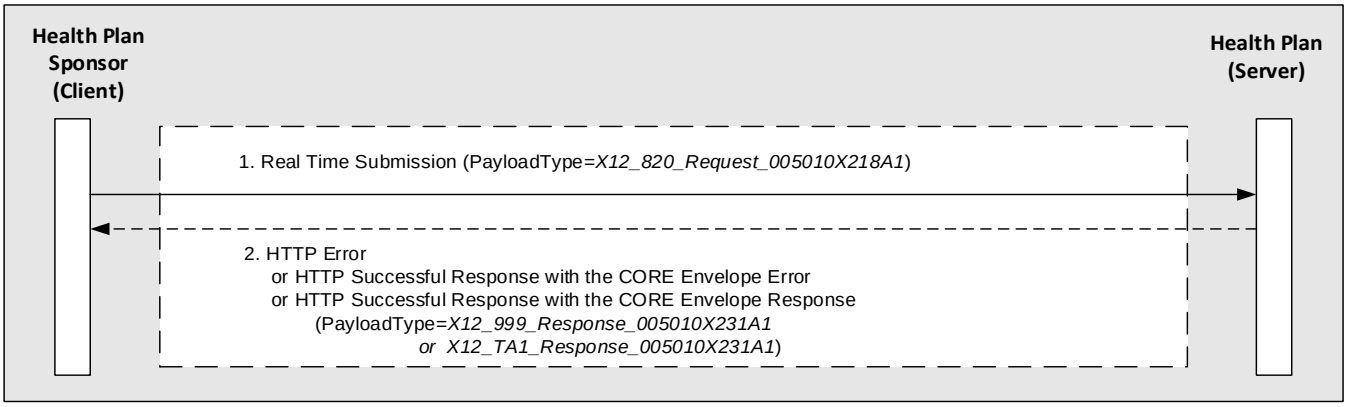
[113] http://en.wikipedia.org/wiki/Transport_Layer_Security

The requester of a Real Time response expects one and only one response on the payload; for example, in the above message interaction, the response payload can only be an ASC X12N v5010 278, or an ASC X12C v5010 999 or an ASC X12C TA1. The following describes the Real Time interaction as shown in the above diagram.

Message Sequence	Description	Reference to Payload Type Table Transaction Name Column in the Processing Modes and Payload Types Document
1	A Healthcare Provider submits a Real Time request to a Health Plan, using PayloadType=*X12_278_Request_005010X217E1_2*.	Health Care Services Review - Request for Review & Response
2	Health Plan responds (synchronously to request message 1) to the request either with an: HTTP Error or HTTP Successful Response with the CORE Envelope Error or HTTP Successful Response with the CORE Envelope Response (PayloadType=*X12_278_Response_005010X217E1_2* or *X12_999_Response_005010X231A1* or *X12_TA1_Response_005010X231A1)*	Health Care Services Review - Request for Review & Response

Example 2: Payroll Deducted and Other Group Premium Payment for Insurance Products (ASC X12N v5010 820)

The UML sequence diagram below shows a *Payroll Deducted and Other Group Premium Payment for Insurance Products* Real Time transaction between a HIPAA-covered Health Plan Sponsor (Client) and a HIPAA-covered Health Plan (Server). The interactions are described in the diagram below.



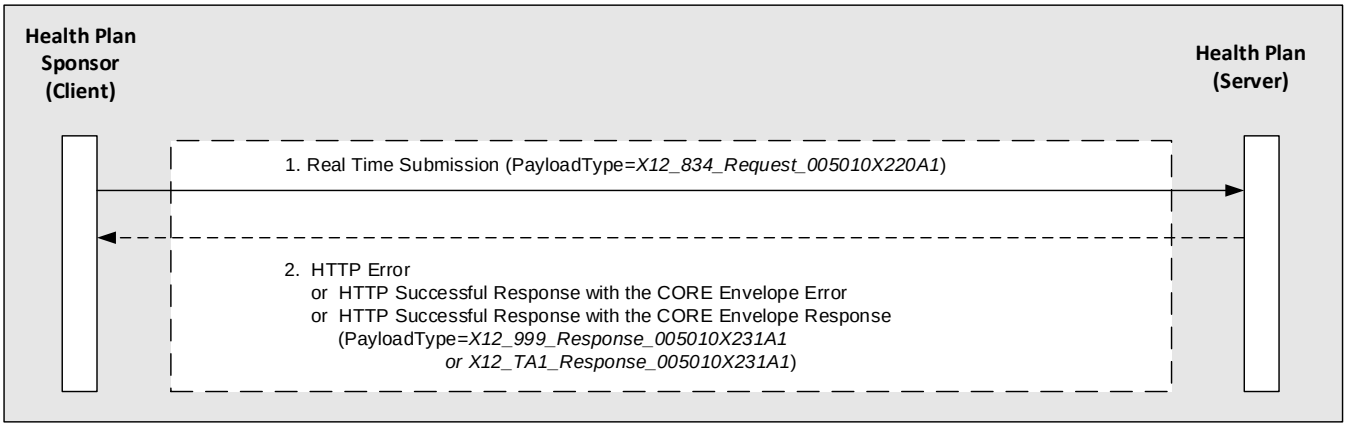
The requester of a Real Time response expects one and only one response on the payload; for example, in the above message interaction, the response payload can only be an ASC X12C v5010 999, or an ASC X12C TA1. The following describes the Real Time interaction as shown in the above diagram.

Message Sequence	Description	Reference to Payload Type Table Transaction Name Column in the Processing Modes and Payload Types Document
1	A Health Plan Sponsor submits a Real Time request to a Health Plan, using PayloadType=*X12_820_Request_005010X218A1*.	Payroll Deducted and Other Group Premium Payment for Insurance Products

Message Sequence	Description	Reference to Payload Type Table Transaction Name Column in the Processing Modes and Payload Types Document
2	A Health Plan responds (synchronously to request message 1) to the request either with an: HTTP Error or HTTP Successful Response with the CORE Envelope Error or HTTP Successful Response with the CORE Envelope Response (PayloadType=*X12_999_Response_005010X231A1 or X12_TA1_Response_005010X231A1*)	Payroll Deducted and Other Group Premium Payment for Insurance Products

Example 3: Benefit Enrollment and Maintenance (ASC X12N v5010 834)

The UML sequence diagram below shows a *Benefit Enrollment and Maintenance* Real Time transaction between a Health Plan Sponsor (Client) and a Health Plan (Server). The interactions are described in the diagram below.

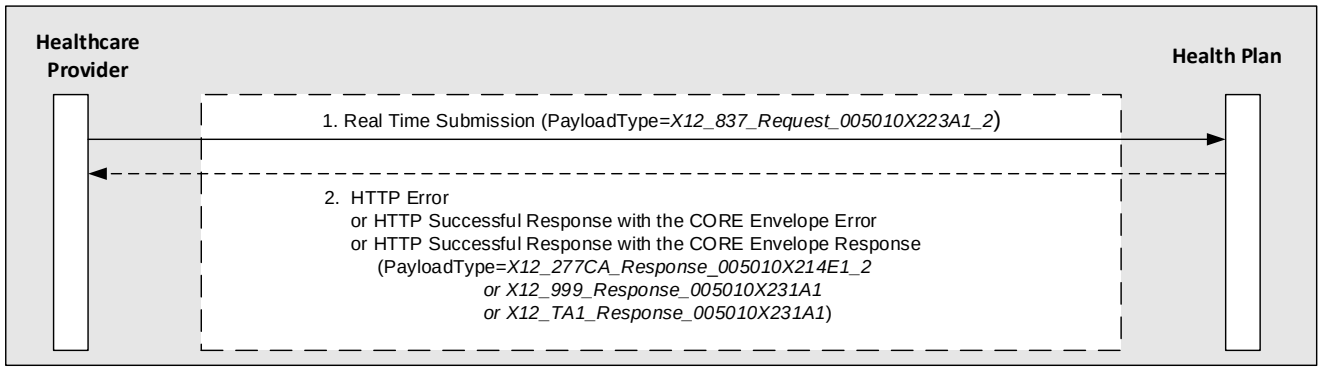


The requester of a Real Time response expects one and only one response on the payload; for example, in the above message interaction, the response payload can only be only an ASC X12C v5010 999, or an ASC X12C TA1. The following describes the Real Time interaction as shown in the above diagram.

Message Sequence	Description	Reference to Payload Type Table Transaction Name Column in the Processing Modes and Payload Types Document
1	A Health Plan Sponsor submits a Real Time request to a Health Plan, using PayloadType=*X12_834_Request_005010X218A1*.	Benefit Enrollment and Maintenance
2	A Health Plan responds (synchronously to request message 1) to the request either with an: HTTP Error or HTTP Successful Response with the CORE Envelope Error or HTTP Successful Response with the CORE Envelope Response (PayloadType=*X12_999_Response_005010X231A1 or X12_TA1_Response_005010X231A1*)	Benefit Enrollment and Maintenance

Example 4: Healthcare Claim (ASC X12N v5010 837 Claim)

The UML sequence diagram below shows an Institutional *Healthcare Claim* Real Time transaction between a HIPAA-covered Healthcare Provider (Client) and a HIPAA-covered Health Plan (Server). The interactions are described in the diagram below.



The requester of a Real Time response expects one and only one response on the payload; for example, in the above message interaction, the response payload can only be an ASC X12N v5010 277CA, or an ASC X12C v5010 999, or an ASC X12C TA1. The following describes the Real Time interaction as shown in the above diagram.

Message Sequence	Description	Reference to Payload Type Table Transaction Name Column in the Processing Modes and Payload Types Document
1	A Health Plan Sponsor submits a Real Time request to a Health Plan, using PayloadType=*X12_837_Request_005010X223A1_2*.	Healthcare Claim: Institutional
2	A Health Plan responds (synchronously to request message 1) to the request either with an: HTTP Error or HTTP Successful Response with the CORE Envelope Error or HTTP Successful Response with the CORE Envelope Response (PayloadType=*X12_277CA_Response_005010X214E1_2* *or X12_999_Response_005010X231A1* *or X12_TA1_Response_005010X231A1*)	Healthcare Claim: Institutional

7.3.2 Batch Interactions

This section describes Batch interactions that include the following steps:

- Submission of Batch Payload (steps 1 and 2 in the diagrams)
- Retrieval of Acknowledgment for the submission (steps 3 and 4 in the diagrams)
- Retrieval of Batch Processing Results (steps 5 and 6 in the diagrams)
- Submission of Acknowledgment for the results retrieved (steps 7 and 8 in the diagrams)

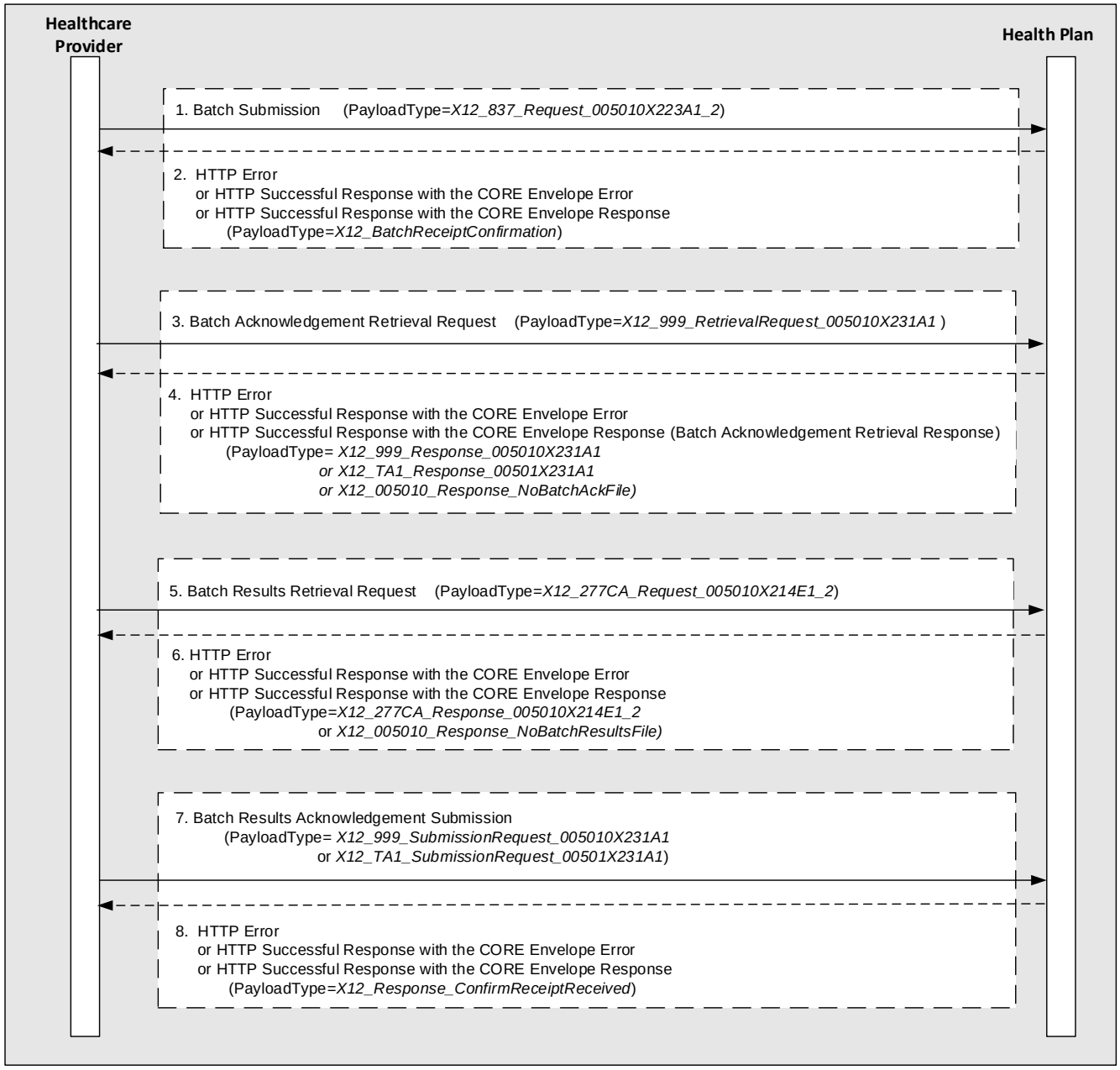
The Batch interactions can be conducted using specific payload types as shown in 7.3.2.1 or with Mixed Payload types as show in 7.3.2.2.

7.3.2.1 ***Batch Interaction for Specific Payload Types***

Within the Batch Interaction for Specific Payload Types, the Batch Payload consists of a single type of transaction set.

Example 1: Health Care Claim (ASC X12N v5010 837 Claim):

The UML sequence diagram below shows a typical Batch Interaction between a HIPAA-covered Healthcare Provider, and a HIPAA-covered Health Plan specifically for ASC X12N v5010 837 batch payloads.



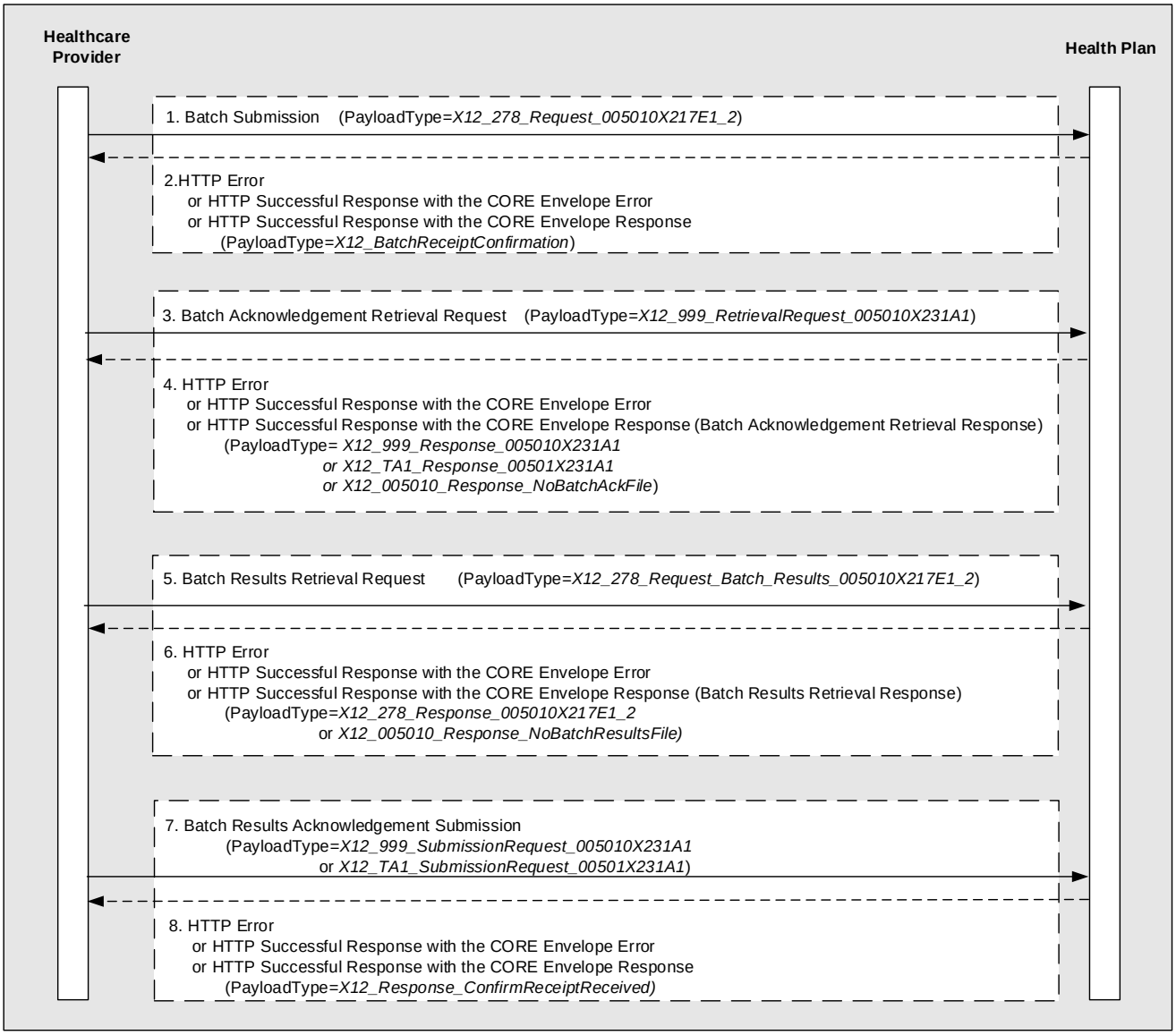
The following describes the Batch interaction as shown in the above diagram.

Message Sequence	Description	Reference to Payload Type Table Transaction Name Column in the Processing Modes and Payload Types Document
1	A Healthcare Provider submits a Batch of requests to a Health Plan, using PayloadType = *X12_837_Request_005010X223A1_2 for an Institutional claim, or X12_837_Request_005010X222A1 for a Professional claim, or X12_837_Request_005010X224A1_2 for a Dental Claim.*	Health Care Claim: Institutional
2	A Health Plan responds (synchronously to request message 1) to the request either with an: HTTP Error or HTTP Successful Response with the CORE Envelope Error or HTTP Successful Response with the CORE Envelope Response (PayloadType=*X12_BatchReceiptConfirmation*)	Batch Receipt Confirmation Response
3	A Healthcare Provider sends a Request to a Health Plan to solicit the acknowledgement (*X12_999_RetrievalRequest_005010X231A1*) for the Batch file that was just submitted.	Implementation Acknowledgement Retrieval
4	A Health Plan responds (synchronously to request message 3) to the request either with an: HTTP Error or HTTP Successful Response with the CORE Envelope Error or HTTP Successful Response with the CORE Envelope Response (Batch Acknowledgement Retrieval Response) (PayloadType= *X12_999_Response_005010X231A1* *or X12_TA1_Response_00501X231A1* *or X12_005010_Response_NoBatchAckFile)*	Implementation Acknowledgement Retrieval
5	A Healthcare Provider sends a Request to a Health Plan to solicit the Health Care Claim Acknowledgement for the batch of claims that was submitted in message sequence 1 using PayloadType=*X12_277CA_Request_005010X214E1_2*.	Health Care Claim Acknowledgement
6	A Health Plan responds (synchronously to request message 5) to the request either with an: HTTP Error or HTTP Successful Response with the CORE Envelope Error or HTTP Successful Response with the CORE Envelope Response (PayloadType=*X12_277CA_Response_005010X214E1_2* or *X12_005010_Response_NoBatchResultsFile)*	Health Care Claim Acknowledgement

Message Sequence	Description	Reference to Payload Type Table Transaction Name Column in the Processing Modes and Payload Types Document
7	A Healthcare Provider submits the acknowledgement Batch Results Acknowledgement Submission (PayloadType= *X12_999_SubmissionRequest_005010X231A1* or *X12_TA1_SubmissionRequest_00501X231A1*) to a Health Plan. This acknowledgment submission is required by the Phase IV CAQH CORE Infrastructure Rule corresponding to the specific transaction.	Implementation Acknowledgement Submission (Request)
8	A Health Plan responds (synchronously to request message 7) to the request either with an: HTTP Error or HTTP Successful Response with the CORE Envelope Error or HTTP Successful Response with the CORE Envelope Response (PayloadType=*X12_Response_ConfirmReceiptReceived*)	Implementation Acknowledgement Submission (Response)

Example 2: Health Care Services Review – Request for Review & Response (ASC X12N v5010 278):

The UML sequence diagram below shows a typical Batch Interaction between a HIPAA-covered Healthcare Provider and a HIPAA-covered Health Plan for ASC X12N v5010 278 batch payloads.



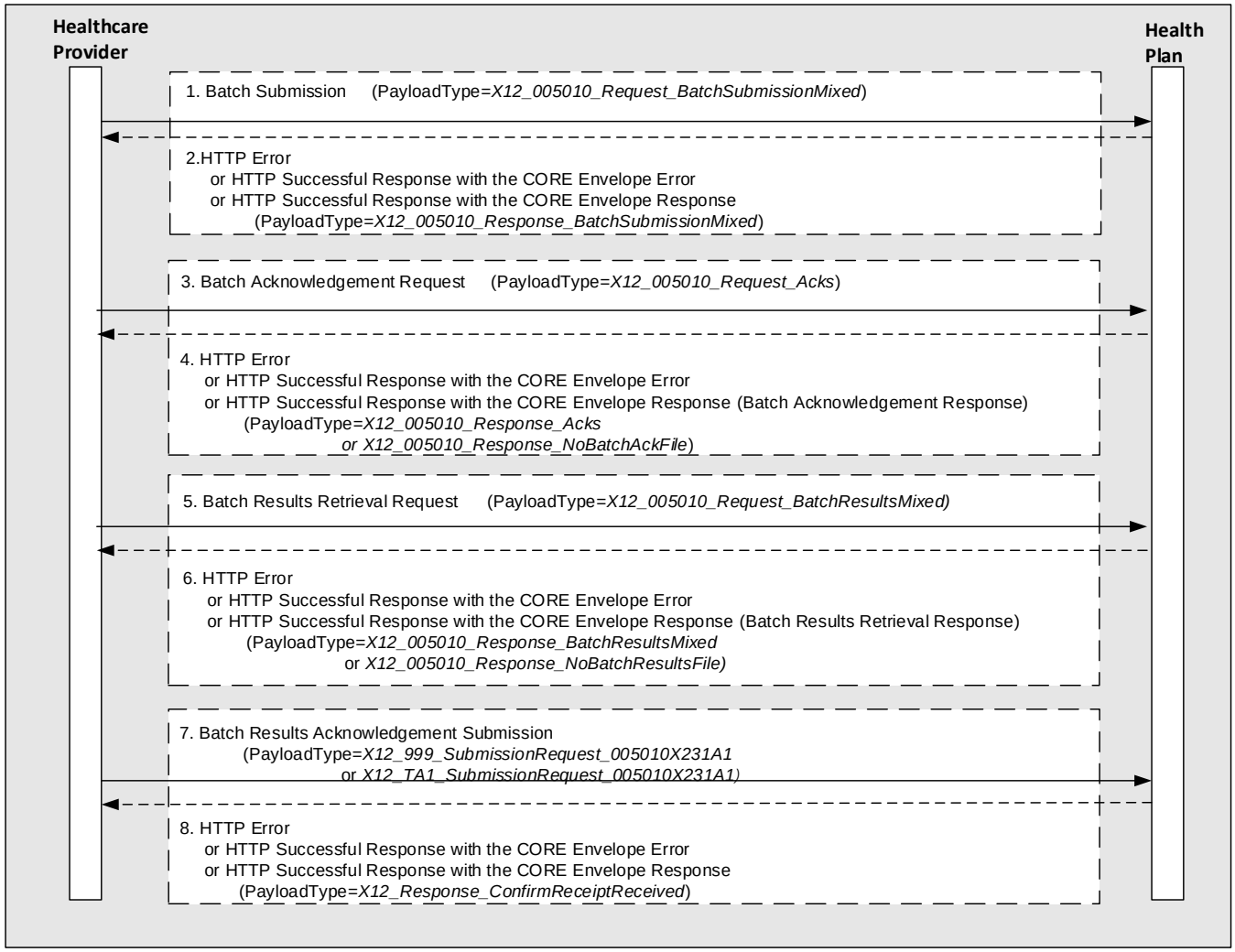
The following describes the Batch interaction as shown in the above diagram.

Message Sequence	Description	Reference to Payload Type Table Transaction Name Column in the Processing Modes and Payload Types Document
1	A Healthcare Provider submits a Batch of requests to a Health Plan, using PayloadType as *X12_278_Request_005010X217E1_2*.	Health Care Services Review – Request for Review & Response
2	A Health Plan responds (synchronously to request message 1) to the request either with an: HTTP Error or HTTP Successful Response with the CORE Envelope Error or HTTP Successful Response with the CORE Envelope Response (PayloadType=*X12_BatchReceiptConfirmation*)	Batch Receipt Confirmation Response

Message Sequence	Description	Reference to Payload Type Table Transaction Name Column in the Processing Modes and Payload Types Document
3	A Healthcare Provider sends a Request to a Health Plan to solicit the acknowledgement (*X12_999_RetrievalRequest_005010X231A1*) for the Batch file that was just submitted.	Implementation Acknowledgement Retrieval
4	A Health Plan responds (synchronously to request message 3) to the request either with an: HTTP Error or HTTP Successful Response with the CORE Envelope Error or HTTP Successful Response with the CORE Envelope Response (Batch Acknowledgement Retrieval Response) (PayloadType= *X12_999_Response_005010X231A1* *or X12_TA1_Response_00501X231A1* *or X12_005010_Response_NoBatchAckFile*)	Implementation Acknowledgement Retrieval
5	A Healthcare Provider sends a Request to a Health Plan to solicit the results of processing the batch that was submitted in message sequence 1, using Payload Type: *X12_278_Request_005010X217E1_2*.	Health Care Services Review – Request for Review & Response
6	A Health Plan responds (synchronously to request message 5) to the request either with an: HTTP Error or HTTP Successful Response with the CORE Envelope Error or HTTP Successful Response with the CORE Envelope Response (Batch Results Retrieval Response) (PayloadType=*X12_278_Response_005010X217E1_2* or *X12_005010_Response_NoBatchResultsFile)*	Health Care Services Review – Request for Review & Response (
7	A Healthcare Provider submits the acknowledgement (PayloadType= *X12_999_SubmissionRequest_005010X231A1*, or *X12_TA1_SubmissionRequest_00501X231A1)* to a Health Plan. This acknowledgment submission is required by CORE Phase I and Phase II Rules.	Implementation Acknowledgement Submission
8	A Health Plan responds (synchronously to request message 7) to the request either with an: HTTP Error or HTTP Successful Response with the CORE Envelope Error or HTTP Successful Response with the CORE Envelope Response (PayloadType=*X12_Response_ConfirmReceiptReceived)*	Implementation Acknowledgement Submission

*7.3.2.2 **Batch Interaction for Mixed Payload Types***

The UML sequence diagram below shows a Mixed Payload Type Batch Interaction between a HIPAA-covered Healthcare Provider and a HIPAA-covered Health Plan.


Healthcare Provider
Health Plan
1. Batch Submission (PayloadType=X12_005010_Request_BatchSubmissionMixed)
2.HTTP Error
or HTTP Successful Response with the CORE Envelope Error
or HTTP Successful Response with the CORE Envelope Response
(PayloadType=X12_005010_Response_BatchSubmissionMixed)
3. Batch Acknowledgement Request (PayloadType=X12_005010_Request_Acks)
4. HTTP Error
or HTTP Successful Response with the CORE Envelope Error
or HTTP Successful Response with the CORE Envelope Response (Batch Acknowledgement Response)
(PayloadType=X12_005010_Response_Acks
or X12_005010_Response_NoBatchAckFile)
5. Batch Results Retrieval Request (PayloadType=X12_005010_Request_BatchResultsMixed)
6. HTTP Error
or HTTP Successful Response with the CORE Envelope Error
or HTTP Successful Response with the CORE Envelope Response (Batch Results Retrieval Response)
(PayloadType=X12_005010_Response_BatchResultsMixed
or X12_005010_Response_NoBatchResultsFile)
7. Batch Results Acknowledgement Submission
(PayloadType=X12_999_SubmissionRequest_005010X231A1
or X12_TA1_SubmissionRequest_005010X231A1)
8. HTTP Error
or HTTP Successful Response with the CORE Envelope Error
or HTTP Successful Response with the CORE Envelope Response
(PayloadType=X12_Response_ConfirmReceiptReceived)

The following describes the typical Mixed Batch interaction as shown in the above diagram.

Message Sequence	Description	Reference to Payload Type Table Transaction Name Column in the Processing Modes and Payload Types Document
1	A Healthcare Provider submits a Batch of requests to a Health Plan, using PayloadType=*X12_005010_Request_BatchSubmissionMixed*)	Batch Submission (mixed payload types)
2	A Health Plan responds (synchronously to request message 1) to the request either with an: HTTP Error or HTTP Successful Response with the CORE Envelope Error or HTTP Successful Response with the CORE Envelope Response (PayloadType=*X12_005010_Response_BatchSubmissionMixed*)	Batch Submission (mixed payload types)
3	A Healthcare Provider sends a Request to a Health Plan with PayloadType=*X12_005010_Request_Acks* to solicit the acknowledgement from a Health Plan (ASC X12C v5010 999 or ASC X12C TA1) for the Batch file that was just submitted.	General Acknowledgements Pick Up
4	A Health Plan responds (synchronously to request message 3) to the request either with an: HTTP Error or HTTP Successful Response with the CORE Envelope Error or HTTP Successful Response with the CORE Envelope Response (Batch Acknowledgement Response) (PayloadType=*X12_005010_Response_Acks or X12_005010_Response_NoBatchAckFile*)	General Acknowledgements Pickup
5	A Healthcare Provider sends a Request to a Health Plan to solicit the Results for the Batch file that was submitted in message sequence 1 using PayloadType=X12_005010_Request_BatchResultsMixed.	Batch Results Retrieval (mixed payload types)
6	A Health Plan responds (synchronously to request message 5) to the request either with an: HTTP Error or HTTP Successful Response with the CORE Envelope Error or HTTP Successful Response with the CORE Envelope Response (Batch Results Retrieval Response) (PayloadType=*X12_005010_Response_BatchResultsMixed or X12_005010_Response_NoBatchResultsFile)*	Batch Results Retrieval (mixed payload types)
7	A Healthcare Provider submits the acknowledgement (PayloadType= *X12_999_SubmissionRequest_005010X231A1* or *X12_TA1_SubmissionRequest_005010X231A1)* to a Health Plan. This acknowledgment submission is required by CORE Phase I and Phase II Rules.	Implementation Acknowledgement Submission

Message Sequence	Description	Reference to Payload Type Table Transaction Name Column in the Processing Modes and Payload Types Document
8	A Health Plan responds (synchronously to request message 7) to the request either with an: HTTP Error or HTTP Successful Response with the CORE Envelope Error or HTTP Successful Response with the CORE Envelope Response (PayloadType=*X12_Response_ConfirmReceiptReceived*)	Implementation Acknowledgement Submission

7.3.3 Generic Batch Interactions

The term *Generic* is used to denote the fact that the Batch Interactions defined herein can be used as building blocks to build more complex interactions if such interactions are needed to support current or future business use cases. Within the Generic Batch Interactions, there are two types:

1) *Generic Push*: this message interaction is characterized by the following steps:
    - Client submits, or "pushes" a Batch Payload to a Server
    - Client then retrieves an acknowledgment (or error) from the Server for the Batch Payload that it had previously submitted to the Server.
2) *Generic Pull*: this message interaction is characterized by the following steps:
    - Client retrieves, or "pulls" a Batch Payload from a Server
    - Client then submits an acknowledgment (or error) to the Server for the Batch Payload that the Client has previously retrieved from the Server.

Both of these message interactions can be used either for Specific Transaction Batch Payload Types (with a single type of transaction set), or for Mixed Batch Payload types (using multiple transaction sets within the same Batch Payload). For simplicity, the examples shown below are limited to Specific Transaction Batch Payload Types.

Two example transactions are shown in the following sub-sections:

a) Benefit Enrollment and Maintenance (ASC X12N v5010 834)

b) Payroll Deducted and Other Group Premium Payment for Insurance Products (ASC X12N v5010 820)

Both of these transactions can use either the *Generic Push* or *Generic Pull* interactions. Depending on the interaction being used, the business actors that use these interactions will need to assume the roles of Client or Server.

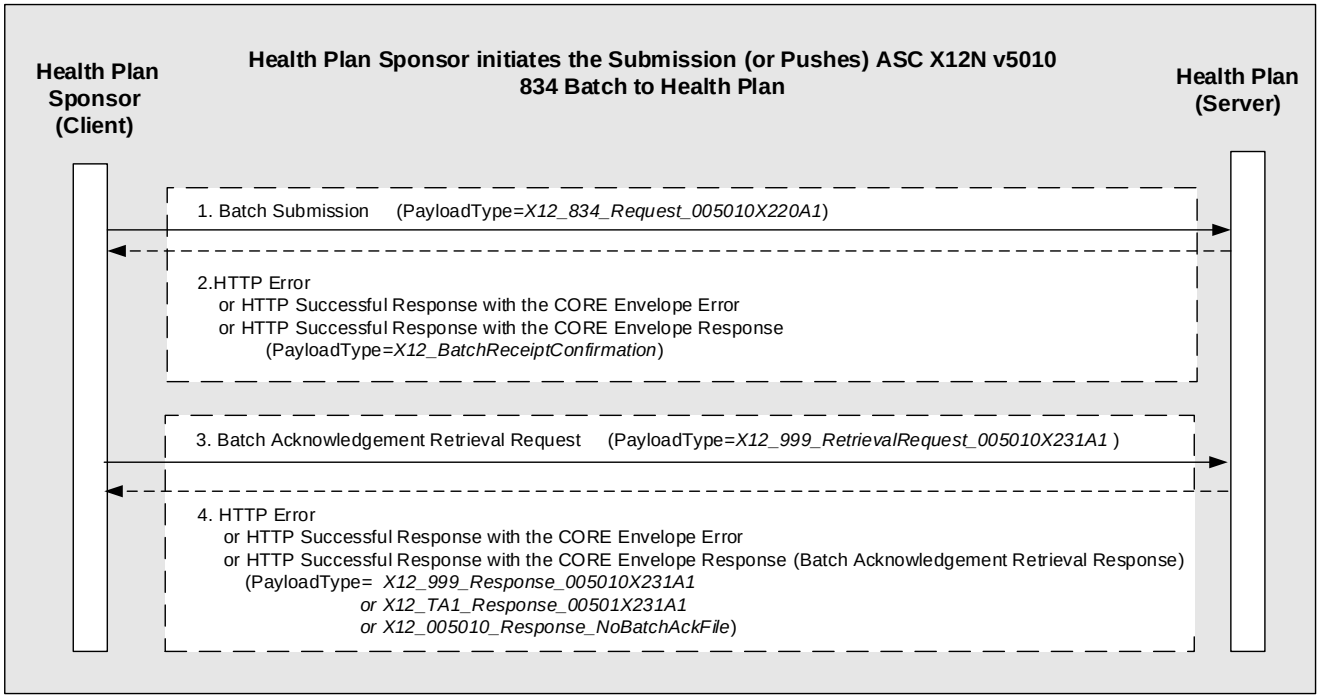
*7.3.3.1 **Generic Push***

This message interaction is characterized by the following steps:

- Client submits, or "pushes" a Batch Payload to a Server
- Client then retrieves an acknowledgment (or error) from the Server for the Batch Payload that it had previously submitted to the Server.

The UML sequence diagrams below show examples of the Generic Push Interactions.

Example: Benefit Enrollment and Maintenance (ASC X12N v5010 834)

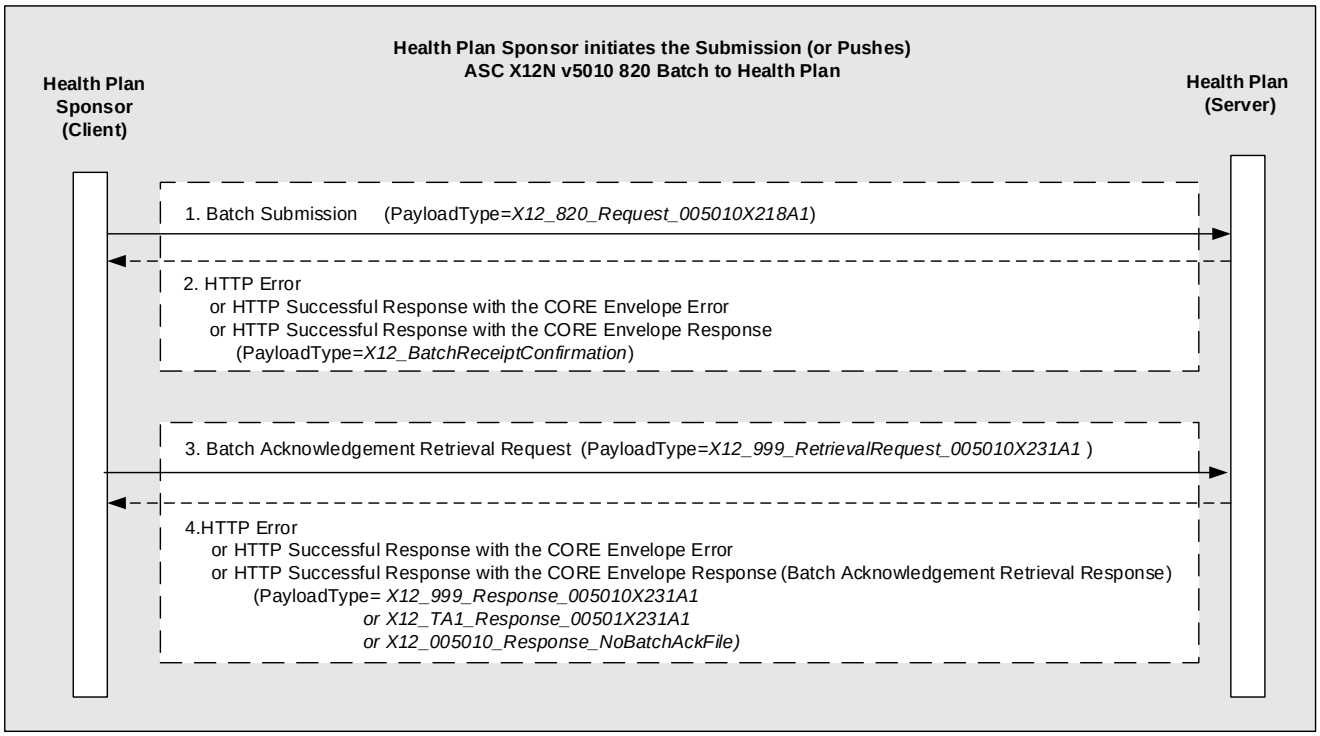


The following describes the *Benefit Enrollment and Maintenance* transaction using the *Generic Push* interaction as shown in the above diagram.

Message Sequence	Description	Reference to Payload Type Table Transaction Name Column in the Processing Modes and Payload Types Document
1	A Health Plan Sponsor (Client) submits to a Health Plan (Server) a Batch of Benefit Enrollment and Maintenance requests using PayloadType=*X12_834_Request_005010X220A1*.	Benefit Enrollment and Maintenance
2	A Health Plan (Server) responds synchronously in Real time either with an: HTTP Error or HTTP Successful Response with the CORE Envelope Error or HTTP Successful Response with the CORE Envelope Response (PayloadType=*X12_BatchReceiptConfirmation*)	Batch Receipt Confirmation Response
3	A Health Plan Sponsor (Client) sends a Request to a Health Plan (Server) with (PayloadType=*X12_999_RetrievalRequest_005010X231A1*) to solicit the acknowledgement (ASC X12C v5010 999 or ASC X12C TA1) for the Batch file that was just submitted.	Implementation Acknowledgement Retrieval

Message Sequence	Description	Reference to Payload Type Table Transaction Name Column in the Processing Modes and Payload Types Document
4	A Health Plan (Server) responds (synchronously to request message 3) to the request either with an: HTTP Error or HTTP Successful Response with the CORE Envelope Error or HTTP Successful Response with the CORE Envelope Response (Batch Acknowledgement Retrieval Response) (PayloadType= *X12_999_Response_005010X231A1* *or X12_TA1_Response_00501X231A1* *or X12_005010_Response_NoBatchAckFile*)	Benefit Enrollment and Maintenance

Example: Payroll Deducted and Other Group Premium Payment for Insurance Products (ASC X12N v5010 820)



The following describes the *Payroll Deducted and Other Group Premium Payment for Insurance Products* transaction using the *Generic Push* interaction, as shown in the above diagram.

Message Sequence	Description	Reference to Payload Type Table Transaction Name Column in the Processing Modes and Payload Types Document
1	The Health Plan Sponsor (Client) submits to a Health Plan (Server) a Batch of Payroll Deducted and Other Group Premium Payment for Insurance Products requests using PayloadType= *X12_820_Request_005010X218A1*.	Payroll Deducted and Other Group Premium Payment for Insurance Products

Message Sequence	Description	Reference to Payload Type Table Transaction Name Column in the Processing Modes and Payload Types Document
2	A Health Plan (Server) responds synchronously in Real time either with an: HTTP Error or HTTP Successful Response with the CORE Envelope Error or HTTP Successful Response with the CORE Envelope Response (PayloadType=*X12_BatchReceiptConfirmation*)	Payroll Deducted and Other Group Premium Payment for Insurance Products
3	A Health Plan Sponsor (Client) sends a Request to a Health Plan (Server) using (PayloadType=*X12_999_RetrievalRequest_005010X231A1*) to solicit the acknowledgement (ASC X12C v5010 999 or ASC X12C TA1) for the Batch file that was just submitted.	Implementation Acknowledgement Retrieval
4	A Health Plan (Server) responds (synchronously to request message 3) to the request either with an: HTTP Error or HTTP Successful Response with the CORE Envelope Error or HTTP Successful Response with the CORE Envelope Response (Batch Acknowledgement Retrieval Response) (PayloadType= *X12_999_Response_005010X231A1* *or X12_TA1_Response_00501X231A1* *or X12_005010_Response_NoBatchAckFile)*	Implementation Acknowledgement Retrieval (Response)

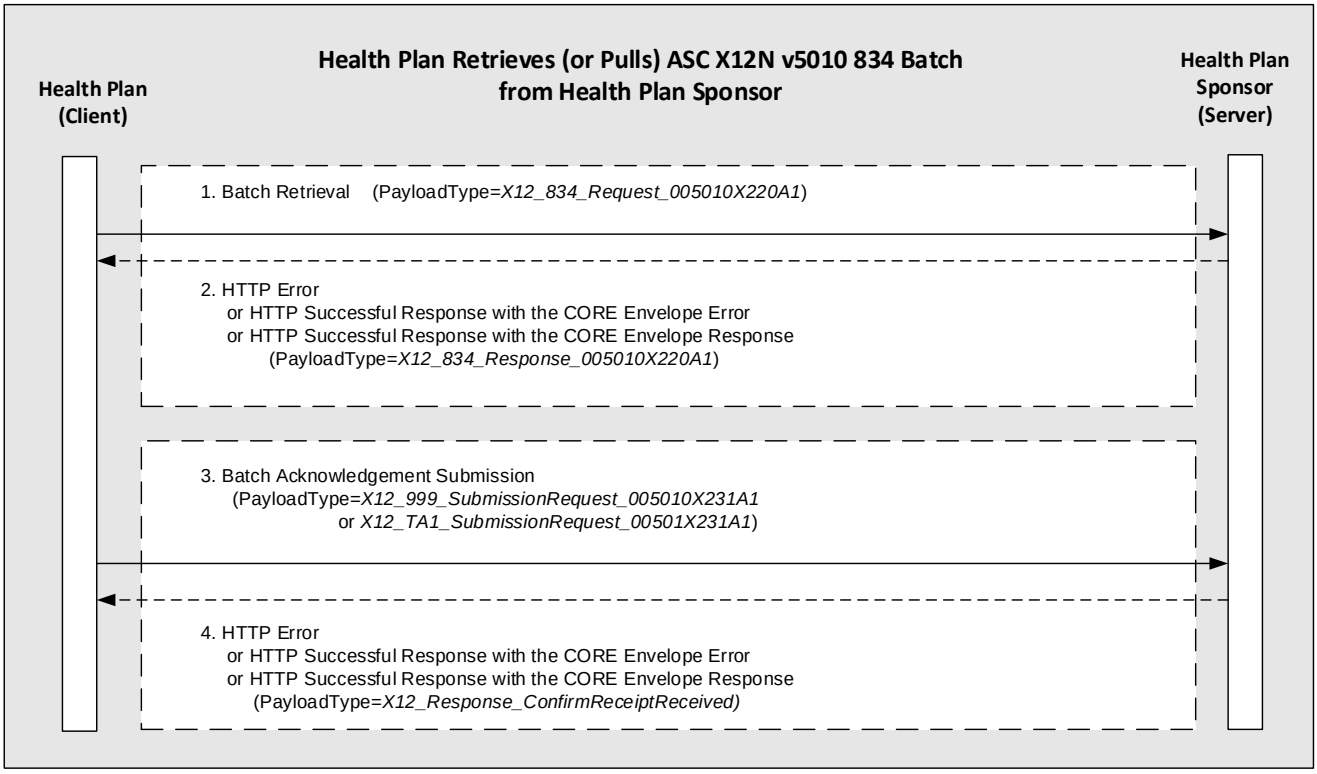
*7.3.3.2 **Generic Pull***

This message interaction is characterized by the following steps:

- Client retrieves, or "pulls" a Batch Payload from a Server
- Client then submits an acknowledgment (or error) to the Server for the Batch Payload that the Client has previously retrieved from the Server.

The UML sequence diagrams below show examples of the *Generic Pull* Interactions.

Example: Benefit Enrollment and Maintenance (ASC X12N v5010 834)

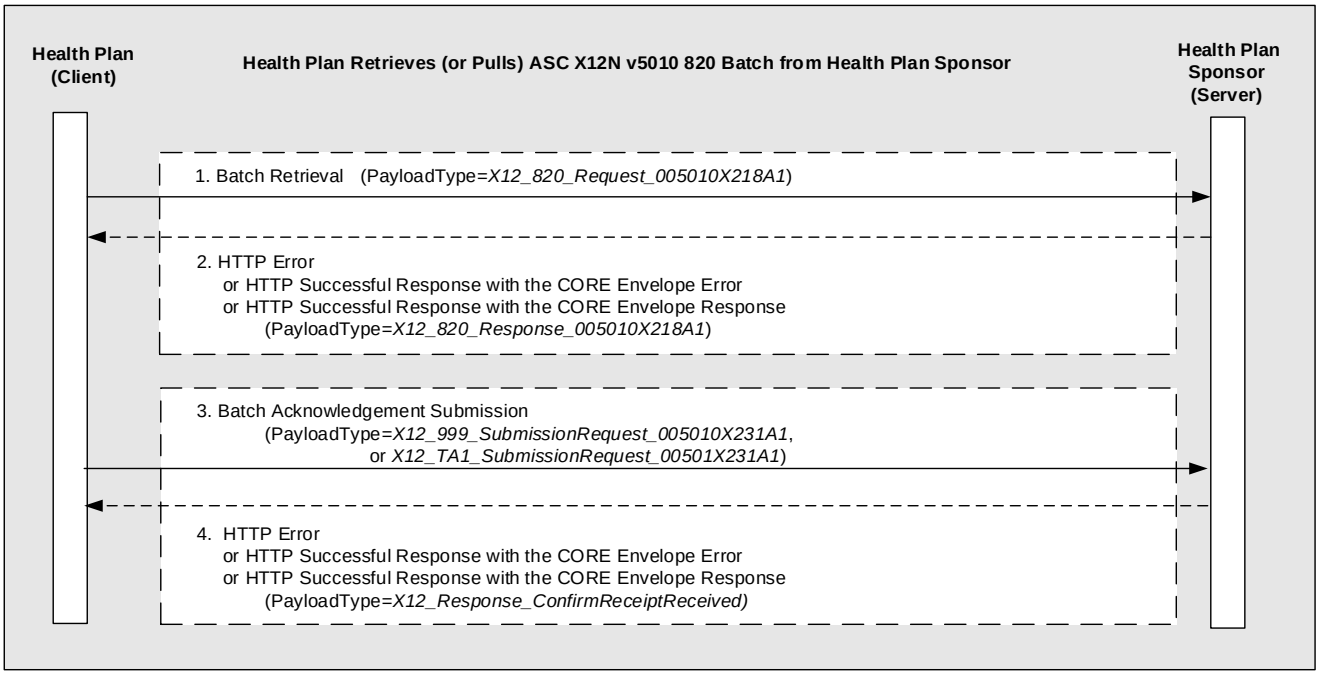


The following describes the *Benefit Enrollment and Maintenance* transaction using the *Generic Pull* interaction, as shown in the above diagram.

Message Sequence	Description	Reference to Payload Type Table Transaction Name Column in the Processing Modes and Payload Types Document
1	A Health Plan (Client) sends a Health Plan Sponsor (Server) a retrieval request for a Batch of Benefit Enrollment and Maintenance requests using PayloadType=*X12_834_Request_005010X220A1*.	Benefit Enrollment and Maintenance:
2	Health Plan Sponsor (Server) responds synchronously in Real time either with an: HTTP Error or HTTP Successful Response with the CORE Envelope Error or HTTP Successful Response with the CORE Envelope Response (PayloadType=*X12_834_Response_005010X220A1*)	Benefit Enrollment and Maintenance:
3	A Health Plan (Client) submits to a Health Plan Sponsor (Server) the acknowledgement (PayloadType *X12_999_SubmissionRequest_005010X231A1* or *X12_TA1_SubmissionRequest_005010X231A1*) to the Health Plan. This acknowledgment submission is required by CORE Phase I and Phase II Rules.	Implementation Acknowledgement Submission

Message Sequence	Description	Reference to Payload Type Table Transaction Name Column in the Processing Modes and Payload Types Document
4	Health Plan Sponsor (Server) responds (synchronously to request message 3) to the request either with an: HTTP Error or HTTP Successful Response with the CORE Envelope Error or HTTP Successful Response with the CORE Envelope Response (PayloadType=*X12_Response_ConfirmReceiptReceived)*	Implementation Acknowledgement Submission

Example: Payroll Deducted and Other Group Premium Payment for Insurance Products (ASC X12N v5010 820)



The following describes the *Payroll Deducted and Other Group Premium Payment for Insurance Products* transaction using the *Generic Pull* interaction, as shown in the above diagram.

Message Sequence	Description	Reference to Payload Type Table Transaction Name Column in the Processing Modes and Payload Types Document
1	A Health Plan (Client) sends a Health Plan Sponsor (Server) a retrieval request for a Batch of *Payroll Deducted and Other Group Premium Payment for Insurance Products* using PayloadType=*X12_820_Request_005010X218A1*.	Payroll Deducted and Other Group Premium Payment for Insurance Products (Retrieval Response)

Message Sequence	Description	Reference to Payload Type Table Transaction Name Column in the Processing Modes and Payload Types Document
2	A Health Plan Sponsor (Server) responds synchronously in Real Time either with an: HTTP Error or HTTP Successful Response with the CORE Envelope Error or HTTP Successful Response with the CORE Envelope Response (PayloadType=*X12_820_Response_005010X218A1*)	Payroll Deducted and Other Group Premium Payment for Insurance Products (Retrieval Response)
3	A Health Plan (Client) submits to a Health Plan Sponsor (Server) the acknowledgement (PayloadType=*X12_999_SubmissionRequest_005010X231A1* or *X12_TA1_SubmissionRequest_005010X231A1*) to a Health Plan. This acknowledgment submission is required by CORE Phase I and Phase II Rules.	Payroll Deducted and Other Group Premium Payment for Insurance Products (Batch Results Acknowledgment Submission)
4	A Health Plan Sponsor (Server) (responds synchronously to request message 3) to the request either with an: HTTP Error or HTTP Successful Response with the CORE Envelope Error or HTTP Successful Response with the CORE Envelope Response (PayloadType=*X12_Response_ConfirmReceiptReceived)*	Payroll Deducted and Other Group Premium Payment for Insurance Products (Batch Results Acknowledgment Response)